UNIVERSITÀ DEGLI STUDI DI PADOVA

Sede Amministrativa: Università degli Studi di Padova

Dipartimento di Matematica Pura ed Applicata

SCUOLA DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE

INDIRIZZO DI MATEMATICA

XXI CICLO

COMPUTING ARITHMETIC SUBGROUPS

OF AFFINE ALGEBRAIC GROUPS

Direttore della Scuola: Ch.mo Prof. Bruno Chiarellotto

Supervisore: Ch.mo Prof. Federico Menegazzo

Dottorando: Dott. Andrea Pavan

UNIVERSITÀ DEGLI STUDI DI PADOVA

Sede Amministrativa: Università degli Studi di Padova

Dipartimento di Matematica Pura ed Applicata

SCUOLA DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE

INDIRIZZO DI MATEMATICA

XXI CICLO

COMPUTING ARITHMETIC SUBGROUPS OF AFFINE ALGEBRAIC GROUPS

Direttore della Scuola: Prof. Bruno Chiarellotto

Supervisori: Prof. Federico Menegazzo e Dott. Willem A. de Graaf

Dottorando: Andrea Pavan

Introduzione

Questo lavoro si occupa di un problema inerente alla teoria algoritmica dei gruppi algebrici affini. Più precisamente, è possibile associare ad ogni gruppo algebrico definito sul campo dei numeri razionali una famiglia di sottogruppi, i cosiddetti sottogruppi aritmetici. Nel 1969, Borel e Harish-Chandra dimostrarono che ogni gruppo aritmetico è finitamente generato. Inoltre, negli anni '80, Grunewald e Segal presentarono un algoritmo che, partendo da un gruppo algebrico "dato esplicitamente" – dove chiaramente è possibile rendere precisa la nozione di "dato esplicitamente" – e un suo sottogruppo aritmetico, calcola un sistema finito di generatori per il gruppo aritmetico. A parte il suo interesse intrinseco, Grunewald e Segal mostrarono che un tale algoritmo può essere impiegato per risolvere un altro importante problema di algebra computazionale, cioè il problema dell'isomorfismo per gruppi nilpotenti finitamente generati. Sfortunatamente, il loro algoritmo è puramente teorico. Infatti, le tecniche impiegate al suo interno lo rendono, da una parte, difficilmente implementabile – a tutt'ora, non è nota alcuna sua implementazione nei principali sistemi di algebra computazionale – e, dall'altra parte, non pratico, nel senso che il suo tempo di esecuzione su un calcolatore come quelli disponibili al giorno d'oggi sarebbe eccessivamente lungo anche per dati d'ingresso relativamente semplici.

In questo lavoro viene considerato il problema di Grunewald e Segal nei due casi particolari in cui il gruppo algebrico è rispettivamente un gruppo unipotente e un toro. Queste ipotesi aggiuntive ci consentono di dare una più precisa descrizione della struttura dei sottogruppi aritmetici, la quale a sua volta conduce sia a una prova indipendente del teorema di Borel e Harish-Chandra, sia a due nuovi algoritmi che risolvono il problema, che ovviamente sono corretti solo per queste particolari classi di gruppi algebrici. Inoltre, gli algoritmi sono stati implementati nei sistemi di algebra computazionale GAP e Magma, e sono stati successivamente testati su alcuni dati d'ingresso. È risultato che essi sono abbastanza efficienti da gestire esempi non banali.

Sul piano tecnico, è conveniente abbandonare il punto di vista dei gruppi algebrici come chiusi di Zariski nello spazio delle matrici quadrate a coefficienti complessi e invertibili – che è stato al contrario adottato nei precedenti lavori – per considerarli piuttosto come varietà "astratte" o, meglio ancora, come schemi gruppali affini. In questo modo si ottiene un'esposizione più elegante ed intrinseca, e in aggiunta è possibile utilizzare la teoria dei quozienti per i gruppi algebrici, che risulta essere molto utile specialmente nel caso unipotente. Inoltre, un ruolo chiave è giocato da due "teoremi di classificazione". Il primo stabilisce un'equivalenza categoriale tra gruppi algebrici unipotenti e algebre di Lie nilpotenti di dimensione finita, e fornisce interessanti informazioni sulla "geometria" di questi gruppi, che possono essere sfruttate anche computazionalmente. Il secondo riduce in un certo senso la teoria dei tori a quella dei gruppi abeliani liberi e finitamente generati su cui agisce un gruppo di Galois. Altre tecniche sono state mutuate dalla teoria dei campi numerici e delle algebre semisemplici, dei gruppi policiclici, e delle basi di Groebner.

La rimanente parte di questo testo è stata redatta in lingua inglese per consentirne la fruibilità ad un numero maggiore di lettori.

Introduction

This work deals with a problem concerning the algorithmic theory of affine algebraic groups. More precisely, it is possible to associate to any algebraic group defined over the field of the rational numbers a family of subgroups, the so-called arithmetic subgroups. In 1969, Borel and Harish-Chandra proved that every arithmetic group is finitely generated. Also, in the '80, Grunewald and Segal presented an algorithm that, starting from an "explicitely given" algebraic group – where of course it is possible to make precise the notion of "explicitely given" – and an arithmetic subgroup of its, computes a finite set of generators for the arithmetic group. Apart from its intrinsic interest, Grunewald and Segal showed that such an algorithm can be employed to solve another important problem of computational algebra, that is to say, the isomorphism problem for finitely generated nilpotent groups. Unfortunately, their algorithm works only in principle. Indeed, the techniques employed in it make the algorithm, on one hand, hard to implement – until now, no implementation on the main computer algebra systems is known – and, on the other hand, not practical, in the sense that its running time on a nowadays available computer would be exceedingly high even for quite simple inputs.

In this work the problem considered by Grunewald and Segal is studied in the two particular cases in which the algebraic group is a unipotent group and a torus, respectively. These supplementary hypothesis enable us to give a more precise description of the structure of the arithmetic subgroups, which in turn leads both to an independent proof of the theorem of Borel and Harsh-Chandra and to two new algorithms solving the problem, which are of course correct only for these particular classes of algebraic groups. Also, the algorithms have been implemented in the computer algebra systems GAP and MAGMA, and they have been successively tested on some inputs. It turns out that they are efficient enough to tackle non trivial examples.

Technically speaking, it is convenient to abandon the point of view of algebraic groups as Zariski-closed subgroups in the space of invertible complex square matrices – which on the contrary was adopted in the previous works – and to regard algebraic groups as "abstract" varieties, or, even better, as affine group schemes. In this way we obtain a more elegant and intrinsic treatment, and in addition it is possible to use the quotient theory for algebraic groups, which turns out to be useful expecially in the unipotent case. Also, a crucial role has been played by two "classification theorems". The first one establishes a categorical equivalence between unipotent algebraic groups and nilpotent finite dimensional Lie algebras, and gives useful information on the "geometry" of these groups, which can also be exploited computationally. The second one reduces, roughly speaking, the theory of tori to the thery of torsion-free finitely generated abelian groups equipped with an action of a Galois group. Other techniques have been taken from the theory of number fields and semisimple algebras, of polycyclic groups, and of Groebner basis.

Chapter 1 contains constructions, results and notations that are used in the following ones. An equivalent formulation of the problem considered by Grunewald and Segal is described in Chapter 2, and two algorithms solving it in the special cases of a unipotent group and of a torus are described in Chapters 3 and 4, respectively. Finally, Chapter 5 contains some remarks.

It should be noticed that, throughout this work, all the algebras are understood to be associative algebras with identity. Also, more information about the computer algebra systems GAP and MAGMA can be found on their websites, which are

`http://www.gap-system.org/`

and

`http://magma.maths.usyd.edu.au/magma/`

respectively.

Ackonwledgements

I would like to thank the Università degli Studi di Trento for its hospitality during the period from October 2007 to November 2008, when most part of this work was carried out.

Contents

Chapter 1

Prerequisites

This chapter contains well known constructions and results that are used in the following ones, without any pretension of completeness. The style of writing is very economical, and there are no proofs. In fact, it is mainly intended to serve as a reference for language and notations, and it is not well suited for a sequential reading. For a better treatment of topics concerning algebraic geometry and algebraic groups, some good references are the classical books [Bo], [Mi], [Mi2] and [Wa]. For the other arguments, some references are indicated in the specific sections.

1.1 Affine algebraic sets and groups

Let k be a field. An affine algebraic set over k is a functor from the category of commutative k-algebras to the category of sets which is naturally isomorphic to the functor represented by a finitely generated algebra. If $\mathbf{X}$ is an affine algebraic set over k, for every algebra R it is customary to denote by $\mathbf{X}(R)$ the set that $\mathbf{X}$ associates to R, and to refer to is as the set of the R-valued points of $\mathbf{X}$. If $\mathbf{Y}$ is another affine algebraic set over k, then a morphism of affine algebraic sets over k from $\mathbf{X}$ to $\mathbf{Y}$ is nothing but a natural transformation. Of course, affine algebraic sets over k and the morphisms between them are the objects and the arrows of a category, respectively, which is called the category of the affine algebraic sets over k. If A is a finitely generated commutative k-algebra, it is customary to denote by $\mathrm{Hom}(A, \bullet)$ the affine algebraic set over k represented by it, and, for every algebra R, to denote by $\mathrm{Hom}(A, R)$ the set of R-valued points of $\mathrm{Hom}(A, \bullet)$. Also, if f is a morphism from A to another finitely generated commutative k-algebra B, then it is customary to denote by $\sharp \circ f$ the morphism from $\mathrm{Hom}(B, \bullet)$ to $\mathrm{Hom}(A, \bullet)$ that to any algebra R associates

$$\mathrm{Hom}(B, R) \to \mathrm{Hom}(A, R) \qquad g \mapsto g \circ f.$$

A very well known fact is that

Proposition 1.1.1 (Yoneda lemma). *There exists a contraviariant functor from the category of finitely generated commutative k-algebras to the category of affine algebraic sets over k that*

- *to every algebra A associates* $\mathrm{Hom}(A, \bullet)$*, and that*

- *to every morphism f associates $\sharp \circ f$.*

It is even an anti-equivalence between the two categories.

An affine algebraic group over k is a functor from the category of commutative k-algebras to the category of groups which is also, once we regard it as a functor to the category of sets, an affine algebraic set over k. Morphisms of affine algebraic groups over k are just natural transformations between them. Of course, affine algebraic groups over k and their morphisms form a category, which is called the category of affine algebraic groups over k. An affine Hopf algebra over k is a finitely generated commutative k-algebra A together with

$$\Delta : A \to A \otimes A, \qquad S : A \to A \qquad \text{and} \qquad \epsilon : A \to k$$

such that

$$\begin{tikzcd} A \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & A \otimes A \arrow[d, "\Delta \otimes \mathrm{id}_A"] \\ A \otimes A \arrow[r, "\mathrm{id}_A \otimes \Delta"'] & A \otimes A \otimes A \end{tikzcd}$$

and

$$\begin{tikzcd} A \arrow[r, "\Delta"] \arrow[dr] & A \otimes A \arrow[d, "\epsilon \otimes \mathrm{id}_A"] \\ & k \otimes A \end{tikzcd}$$

and, finally,

$$\begin{tikzcd} A \arrow[r, "\epsilon"] \arrow[d, "\Delta"'] & k \arrow[d] \\ A \otimes A \arrow[r] & A \end{tikzcd}$$

are commutative, where the diagonal arrow in the second diagram is the canonical isomorphism, and, in the third diagram, the bottow row is the composition of $S \otimes \mathrm{id}_A$ with the unique morphism from $A \otimes A$ to A sending every $a \otimes b$ to ab, and the right column is the map sending every α to $\alpha \cdot 1_A$. If this is the case, Δ is called the co-multiplication of A, and S and ϵ are the co-inverse and the co-identity of A, respectively. Also, if A' is another Hopf algebra over k, a morphism f of Hopf algebras from A to A' is a morphism of k-algebras such that

$$\Delta' \circ f = f \otimes f \circ \Delta, \qquad S' \circ f = f \circ S \qquad \text{and} \qquad \epsilon' = f \circ \epsilon \ ,$$

where Δ', S' and ϵ' are the co-multiplication, the co-inverse and the co-identity of A', respectively. Of course, affine Hopf algebras over k and their morphisms form a category, which is called the category of affine Hopf algebras over k. If A is an affine Hopf algebra over k, there exists a unique affine algebraic group over k whose underlying affine algebraic set is $\mathrm{Hom}(A, \bullet)$ and that to every k-algebra R associates the group whose multiplication is given by

$$(x, y) \mapsto \mu \circ x \otimes y \circ \Delta \ ,$$

where Δ is the co-multiplication of A and μ is the unique morphism from $A \otimes A$ to A sending $a \otimes b$ to ab, whose inverse is given by

$$x \mapsto x \circ S \ ,$$

where S is the co-inverse of A, and whose identity is the composition of

$$A \xrightarrow{\epsilon} k \to R \ ,$$

where ϵ is the co-identity of A and the map on the right sends every α to $\alpha \cdot 1_A$. It is customary to denote it by $\mathrm{Hom}(A, \bullet)$. We will refer to it as the affine algebraic group over k represented by A. It is well known that

Proposition 1.1.2. *There exists a contravariant functor from the category of affine Hopf algebras over k to the category of affine algebraic groups over k that*

- *to every Hopf algebra A associates* $\mathrm{Hom}(A, \bullet)$*, and that*
- *to every morphism f associates $\sharp \circ f$.*

It is even an anti-equivalence of categories.

We say that a morphism η of affine algebraic groups over k is a monomorphism if it is so once we regard it as an arrow in the category of affine algebraic groups over k. It is well known that this is the case if and only if for every k-algebra R the map that η associates to R is injective. Also, if $\mathbf{G}$ is an affine algebraic groups over k, an algebraic subgroup of $\mathbf{G}$ is an affine algebraic group $\mathbf{H}$ over k such that,

- once we regard both $\mathbf{H}$ and $\mathbf{G}$ as functors to the category of sets, $\mathbf{H}$ is a subfunctor of $\mathbf{G}$, and that,
- for every k-algebra R, the inclusion of $\mathbf{H}(R)$ into $\mathbf{G}(R)$ is a group morphism.

If this is the case, the inclusion of $\mathbf{H}$ into $\mathbf{G}$ is a monomorphism. Similarly, we say that η is an epimorphism or an isomorphism if it is so as an arrow, and it is easy to show that η is an isomorphism if and only if for every k-algebra R the map that η associates to R is bijective. Further, we say that another morphism ζ of affine algebraic groups over k is a kernel or an image of η if it is so once we regard both ζ and η as arrows in the category of affine algebraic groups over k. Also, let us denote by $\mathbf{G}$ and by $\mathbf{H}$ the domain and the codomain of η, respectively. It is well known that there exists a unique subfunctor $\mathbf{N}$ of $\mathbf{G}$ that to every k-algebra R associates the kernel – in the usual, set-theoretical sense – of the group morphism which is associated to R by η, and it is the unique algebraic subgroup of $\mathbf{G}$ such that its inclusion in $\mathbf{G}$ is a kernel of η. We refer to $\mathbf{N}$ and to its inclusion in $\mathbf{G}$ as *the* kernel of η. Similarly, there exists a unique algebraic subgroup $\mathbf{K}$ of $\mathbf{H}$ such that its inclusion in $\mathbf{H}$ is an image of η. We will refer to $\mathbf{K}$ and to its inclusion in $\mathbf{H}$ as the image of η. Also, if $\mathbf{G}$ is an affine algebraic group over k, A is a finitely generated commutative k-algebra and η is a natural isomorphism from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$, then we say that $\mathbf{G}$ is connected if A is an integral domain. Of course, by Yoneda lemma this is a good definition. Further, by Noether normalization theorem, A contains a finite set S such that the sub-k-algebra $k[S]$ of A generated by S is a polynomial algebra on S, and that A is a finitely generated $k[S]$-module. Although S is in general not unique, its cardinality in an invariant. Thus it makes sense to define the dimension of $\mathbf{G}$ as the cardinality of S. The dimension of an affine algebraic group has many nice properties. In particular, if φ is a morphism with domain $\mathbf{G}$, kernel $\mathbf{N}$ and image $\mathbf{Q}$, then the dimension of $\mathbf{G}$ is the sum of the dimensions of $\mathbf{N}$ and $\mathbf{Q}$.

1.2 Tensor product and scalars extension

Let k be a field, and R a commutative k-algebra. If V and W are finite dimensional k-vector spaces, and f is a linear transformation from V to W, then there exists a unique map $\tilde{f}$ from $R \otimes V$ to $R \otimes W$ such that

- it is a morphism of R-modules with respect to the canonical structure of R-module on both $R \otimes V$ and $R \otimes W$, and that
-
$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "1\otimes \mathrm{id}_V"'] & W \arrow[d, "1\otimes \mathrm{id}_W"] \\ R\otimes V \arrow[r, "\tilde{f}"] & R\otimes W \end{tikzcd}$$

  is commutative.

We will refer to it as the morphism obtained from f extending scalars to R. If U is another finite dimensional k-vector space and f is now a bilinear map from the catesian product of U and V to W, then there exists a unique map $\tilde{f}$ from the cartesian product of $R \otimes U$ and $R \otimes V$ to $R \otimes W$ such that

- it is a bilinear map of R-modules with respect to the canonical structure of R-module on $R \otimes U$, $R \otimes V$ and $R \otimes W$, and that
-
$$\begin{tikzcd} U\times V \arrow[r, "f"] \arrow[d, "(1\otimes \mathrm{id}_U)\times(1\otimes \mathrm{id}_V)"'] & W \arrow[d, "1\otimes \mathrm{id}_W"] \\ R\otimes U\times R\otimes V \arrow[r, "\tilde{f}"] & R\otimes W \end{tikzcd}$$

  is commutative.

We will refer to it as the bilinear map obtained from f extending scalars to R. A standard reference for these and other properties of tensor products is [AMD].

1.3 Vector spaces as algebraic groups

Let k be a field, and V a finite dimensional k-vector space. There exists a functor $\bullet \otimes V$ from the category of commutative k-algebras to the category of groups such that

- to every algebra R associates the additive group of $R \otimes V$, and
- to every morphism f from R to S associates $f \otimes \mathrm{id}_V$.

It is called the affine space on V. Also, it is even an affine algebraic group over k. In fact, let us denote by $\mathrm{S}(V^*)$ the symmetric algebra on the dual space of V. Of course, it is finitely generated. Also, the family of maps that to any algebra R associates the map from $R \otimes V$ to $\mathrm{Hom}(\mathrm{S}(V^*), R)$ that in turn sends every $a \otimes x$ to the unique morphism of algebras f from $\mathrm{S}(V^*)$ to R such that

$$\begin{tikzcd} V^* \arrow[r] \arrow[d] & R \\ \mathrm{S}(V^*) \arrow[ur, "f"] & \end{tikzcd}$$

is commutative, where the vertical arrow is the canonical map and the horizontal arrow is the map sending any λ to $\lambda(x)a$, is a natural isomorphism from $\bullet \otimes V$ to $\mathrm{Hom}(\mathrm{S}(V^*), \bullet)$. We will often refer to it as the canonical natural isomorphism. Also, $\mathrm{S}(V^*)$ is endowed with a structure of Hopf algebra over k, whose co-multiplication is the unique map sending any $x \in V^*$ to $x \otimes 1 + 1 \otimes x$, whose co-inverse is the unique map sending any $x \in V^*$ to $-x$ and whose co-identity is the unique map sending any $x \in V^*$ to 0. We will refer to it as the canonical Hopf algebra structure on $\mathrm{S}(V^*)$. It is well-known that the canonical natural isomorphism between $\bullet \otimes V$ and $\mathrm{Hom}(\mathrm{S}(V^*), \bullet)$ is a morphism of algebraic groups with respect to the structure of affine algebraic group on $\mathrm{Hom}(\mathrm{S}(V^*), \bullet)$ corresponding to the canonical structure of Hopf algebra on $\mathrm{S}(V^*)$.

Now let W be another finite dimensional k-vector space, and let f be a linear transformation from V to W. Then there exists a natural transformation from $\bullet \otimes V$ to $\bullet \otimes W$ that to any algebra R associates the morphism of R-modules from $R \otimes V$ to $R \otimes W$ obtained from f extending scalars to R. We will refer to it as the natural transformation associated to f.

1.4 Endomorphisms, matrices, algebraic groups

Let V be a finite dimensional vector space over k. There exists a functor $\mathrm{End}(\bullet \otimes V)$ from the category of commutative k-algebras to the category of groups such that

- to every algebra R associates the additive group $\mathrm{End}(R \otimes V)$ of the endomorphisms of the R-module $R \otimes V$, and
- to every morphism f from R to S associates the map which in turn sends any endomorphism φ of $R \otimes V$ to the unique endomorphism ψ of $S \otimes V$ such that

$$\begin{tikzcd} R \otimes V \arrow[r, "\varphi"] \arrow[d, "f \otimes \mathrm{id}_V"'] & R \otimes V \arrow[d, "f \otimes \mathrm{id}_V"] \\ S \otimes V \arrow[r, "\psi"] & S \otimes V \end{tikzcd}$$

  is commutative.

It turns out that it is even an affine algebraic group over k. In fact, let us denote by $\bullet \otimes \mathrm{End}(V)$ the affine space on $\mathrm{End}(V)$. Then the family of maps that to every algebra R associates the map from $R \otimes \mathrm{End}(V)$ to $\mathrm{End}(R \otimes V)$, which in turn sends any $a \otimes \varphi$ to the endomorphism of $R \otimes V$ sending $b \otimes x$ to $ab \otimes \varphi(x)$, is a natural isomorphism from $\bullet \otimes \operatorname{End}(V)$ to $\operatorname{End}(\bullet \otimes V)$. We will often refer to it as the canonical natural isomorphism. Also, let us denote by $\mathrm{S}(\operatorname{End}(V)^*)$ the symmetric algebra on the dual space of $\operatorname{End}(V)$. Composing the canonical natural isomorphism between $\operatorname{Hom}(\mathrm{S}(\operatorname{End}(V)^*), \bullet)$ and $\bullet \otimes \operatorname{End}(V)$ with the canonical natural isomorphism between $\bullet \otimes \operatorname{End}(V)$ and $\operatorname{End}(\bullet \otimes V)$, we obtain a natural isomorphism from $\operatorname{Hom}(\mathrm{S}(\operatorname{End}(V)^*), \bullet)$ to $\operatorname{End}(\bullet \otimes V)$. Again, we will refer to it as the canonical natural isomorphism.

Similarly, it makes sense to consider the functor GL_V from the category of commutative k-algebras to the category of groups such that

- to any algebra R associates the group $\mathrm{GL}_V(R)$ of the automorphisms of the R-module $R \otimes V$, and
- to any morphism f from R to S associates the map that in turn sends any automorphism φ of $R \otimes V$ to the unique automorphism ψ of $S \otimes V$ such that

$$\begin{array}{ccc} R \otimes V & \xrightarrow{\varphi} & R \otimes V \\ {\scriptstyle f\otimes \mathrm{id}_V}\downarrow & & \downarrow{\scriptstyle f\otimes \mathrm{id}_V} \\ S \otimes V & \xrightarrow{\psi} & S \otimes V \end{array}$$

  is commutative.

Of course, it is a subfunctor of $\operatorname{End}(\bullet \otimes V)$. Also, it is well-known that it is even an affine algebraic group over k, which is called the general linear group on V.

Now let m be an integer greater than 1. There exists a functor M_m from the category of commutative k-algebras to the category of groups such that

- to every algebra R associates the additive group $\mathrm{M}_m(R)$ of square matrices of order m with coefficients in R, and
- to every morphism f from R to S associates the map given by

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \mapsto \begin{pmatrix} f(a_{11}) & \cdots & f(a_{1m}) \\ \vdots & & \vdots \\ f(a_{m1}) & \cdots & f(a_{mm}) \end{pmatrix}.$$

It turns out that it is even an affine algebraic group over k. In fact, let us denote by $\hat{X}$ the set of indeterminates X_{ij} where i and j are integers between 1 and m, and by $k[\hat{X}]$ the polynomial algebra with rational coefficients in the indeterminates in $\hat{X}$. Of course, $k[\hat{X}]$ is finitely generated. Also, the family of maps that to every algebra R associates the map from $\operatorname{Hom}(k[\hat{X}], R)$ to $\mathrm{M}_m(R)$ which in turn sends φ to

$$\begin{pmatrix} \varphi(X_{11}) & \cdots & \varphi(X_{1m}) \\ \vdots & & \vdots \\ \varphi(X_{m1}) & \cdots & \varphi(X_{mm}) \end{pmatrix},$$

is a natural isomorphism from $\operatorname{Hom}(k[\hat{X}], \bullet)$ to M_m. We will refer to it as the canonical natural isomorphism.

Similarly, it makes sense to consider the functor GL_m from the category of commutative k-algebras to the category of groups such that

- to every algebra R associates the group $\mathrm{GL}_m(R)$ of the invertible square matrices of order m with coefficients in R, and
- to every morphism f from R to S associates the map that

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \mapsto \begin{pmatrix} f(a_{11}) & \cdots & f(a_{1m}) \\ \vdots & & \vdots \\ f(a_{m1}) & \cdots & f(a_{mm}) \end{pmatrix}.$$

Of course, it is a subfunctor of M_m. Also, it turns out that it is even an affine algebraic group over k. More precisely, let us put

$$\det = \sum_{\sigma \in S_m} \mathrm{sgn}(\sigma) X_{1\sigma(1)} \cdots X_{m\sigma(m)},$$

where S_m is the symmetric group on $\{1, \ldots, m\}$ and sgn is the sign morphism, and let us denote by $k[\hat{X}]_{\det}$ the localization of $k[\hat{X}]$ at det. Of course, $k[\hat{X}]_{\det}$ is finitely generated. Also, the family of maps that to any algebra R associates the map from $\mathrm{Hom}(k[\hat{X}]_{\det}, R)$ to $\mathrm{GL}_m(R)$ which in turn sends any morphism φ to

$$\begin{pmatrix} \varphi(X_{11}) & \cdots & \varphi(X_{1m}) \\ \vdots & & \vdots \\ \varphi(X_{m1}) & \cdots & \varphi(X_{mm}) \end{pmatrix},$$

is a natural isomorphism from $\mathrm{Hom}(k[\hat{X}]_{\det}, \bullet)$ to GL_m. We will often refer to it as the canonical natural isomorphism. Further,

$$\begin{tikzcd} \mathrm{Hom}(k[\hat{X}]_{\det}, \bullet) \arrow[r, "\sharp\circ\lambda"] \arrow[d] & \mathrm{Hom}(k[\hat{X}], \bullet) \arrow[d] \\ \mathrm{GL}_m \arrow[r] & \mathrm{M}_m \end{tikzcd}$$

is commutative, where λ is the localization map from $k[\hat{X}]$ to $k[\hat{X}]_{\det}$, the bottom row is the inclusion and the vertical rows are the canonical natural isomorphisms.

Now suppose that V has dimension m, and let $x_1, \ldots, x_m$ be a basis of V. For every i and j between 1 and m, let us denote by e_{ij} the unique endomorphism of V sending x_i to x_j and all the other elements of the given basis of V to 0. Of course, the set of the e_{ij} for i and j between 1 and m is a basis for $\mathrm{End}(V)$. Let us denote by e_{ij}^* the elements of the basis for $\mathrm{End}(V)^*$ which is dual to it. Clearly, there exists a unique morphism of k-algebras from $k[\hat{X}]$ to $\mathrm{S}(\mathrm{End}(V)^*)$ sending every X_{ij} in X to e_{ij}^*, and it is an isomorphism. We will refer to it as the algebras isomorphism from $k[\hat{X}]$ to $\mathrm{S}(\mathrm{End}(V)^*)$ with respect to $x_1, \ldots, x_m$. Also, the family of maps that to any algebra R associates the map from $\mathrm{End}(R \otimes V)$ to $\mathrm{M}_m(R)$ that in turn sends any endomorphism of $R \otimes V$ to its matrix with respect to the basis $1_R \otimes x_1, \ldots, 1_R \otimes x_m$, is a natural isomorphism from $\mathrm{End}(\bullet \otimes V)$ to M_m. We will refer to it as the natural isomorphism with respect to $x_1, \ldots, x_m$. Further,

$$\begin{tikzcd} \mathrm{Hom}(\mathrm{S}(\mathrm{End}(V)^*), \bullet) \arrow[r, "\sharp\circ i"] \arrow[d] & \mathrm{Hom}(k[\hat{X}], \bullet) \arrow[d] \\ \mathrm{End}(\bullet \otimes V) \arrow[r] & \mathrm{M}_m \end{tikzcd}$$

is commutative, where i is the isomorphism from $k[\hat{X}]$ to $\mathrm{S}(\mathrm{End}(V)^*)$ with respect to $x_1, \ldots, x_m$, the bottom row is the natural isomorphism with respect to $x_1, \ldots, x_m$ and the columns are the canonical natural isomorphisms. Finally, there exists a unique natural transformation from GL_V to GL_m such that

$$\begin{tikzcd} \mathrm{GL}_V \arrow[r] \arrow[d] & \mathrm{GL}_m \arrow[d] \\ \mathrm{End}(\bullet \otimes V) \arrow[r] & \mathrm{M}_m \end{tikzcd}$$

is commutative, where the columns are the inclusions and the bottom row is the natural isomorphism with respect to $x_1, \ldots, x_m$, and it is a natural isomorphism. Again, we will refer to it as the natural isomorphism with respect to $x_1, \ldots, x_m$.

Now let $\mathbf{G}$ be an affine algebraic group over k. A linear representation, or an action, of $\mathbf{G}$ on V is a natural transformation ρ from the cartesian product of $\mathbf{G}$ and the affine space $\bullet \otimes V$ on V to $\bullet \otimes V$ itself such that for every algebra R,

$$\rho_R : \mathbf{G}(R) \times R \otimes V \to R \otimes V,$$

that ρ associates to R, is an action of $\mathbf{G}(R)$ on $R \otimes V$ as automorphisms of R-modules. A subspace W of V is stable under ρ if for every algebra R, every $g \in \mathbf{G}(R)$ and every $x \in R \otimes W$, we have that $\rho_R(g, x) \in R \otimes W$. If this is the case, thexe exists a unique action ρ' of $\mathbf{G}$ on W such that for any algebra R, any $g \in \mathbf{G}(R)$ and any $x \in R \otimes W$, we have that

$$\rho'(g, x) = \rho(g, x).$$

Similarly, there exists a unique action ρ'' of $\mathbf{G}$ on V/W such that for any algebra R, any $g \in \mathbf{G}(R)$ and any $x \in R \otimes V$, we have that

$$\rho''(g, \pi_R(x)) = \pi_R(\rho(g, x)).$$

where π_R is the map obtained from the canonical projection of V onto V/W extending scalars to R. Therefore, if W is a ρ-stable subspace of V, then $\mathbf{G}$ acts on W and on V/W, too. Also, if V' is another finite dimensional k-vector space, and ρ' is now an action of $\mathbf{G}$ on W, then there exists a unique action ρ'' of $\mathbf{G}$ on $V \oplus V'$ such that for every algebra R, every $g \in \mathbf{G}(R)$, every $x \in R \otimes V$ and every $x' \in R \otimes V'$,

$$\rho''_R(g, \iota_R(x)) = \iota_R(\rho_R(g, x)) \quad \text{and} \quad \rho''_R(g, \iota'_R(x')) = \iota'_R(\rho'_R(g, x')) \ ,$$

where ι_R and ι'_R are the maps obtained from the canonical injection of V and of V' into $V \oplus V'$ extending scalars to R, respectively. Therefore $\mathbf{G}$ acts on the direct sum of V and of V', too. Further, we say that $x \in V$ is stable under the action of ρ if for every algebra R, $1_R \otimes x$ is stable under ρ_R. If ρ is an action of $\mathbf{G}$ on V, then the family of maps that to any algebra R associates the map from $\mathbf{G}(R)$ to $\mathrm{GL}_V(R)$ which in turn sends any g to the automorphism of $R\otimes V$ sending any x to $\rho_R(g,x)$, is a morphism of algebraic groups, and in this way we obtain a bijection between linear representations of $\mathbf{G}$ on V and morphisms of algebraic groups from $\mathbf{G}$ to GL_V. We say that an action of $\mathbf{G}$ on V is faithful if the corresponding morphism from $\mathbf{G}$ to GL_V is a monomorphism. Also, the kernel and the image of an action of $\mathbf{G}$ on V are the kernel and the image of the corresponding morphism from $\mathbf{G}$ to GL_V. The composition of the morphism from $\mathbf{G}$ to GL_V corresponding to ρ with the natural isomorphism from GL_V to GL_m with respect to $x_1, \ldots, x_m$, is a morphism of algebraic groups from $\mathbf{G}$ to GL_m, and in this way we obtain a bijection between linear representations of $\mathbf{G}$ on V and morphisms of algebraic groups from $\mathbf{G}$ to GL_m. We refer to the morphism from $\mathbf{G}$ to GL_m obtained from ρ in this way as the morphism corresponding to ρ with respect to $x_1, \ldots, x_m$. Of course, an action of $\mathbf{G}$ on V is faithful if and only if the corresponding morphism of algebraic groups from $\mathbf{G}$ to GL_m with respect to $x_1, \ldots, x_m$ is a monomorphism. If $\mathbf{G}$ is an algebraic subgroup of GL_m, we will refer to the action of $\mathbf{G}$ on k^m corresponding to the inclusion of $\mathbf{G}$ into GL_m with respect to the canonical basis of k^m as the canonical action.

A basic fact is that

Proposition 1.4.1. *For any algebraic group* $\mathbf{G}$ *over* k*, there exists a monomorphism of algebraic groups from* $\mathbf{G}$ *into some* GL_m.

Two immediate consequences of the proposition above are that every affine algebraic group over $\mathbb{Q}$ is isomorphic to an algebraic subgroup of some GL_m, and that it admits a faithful linear representation on some k^m.

1.5 Multiplicative group of an algebra

Let A be a finite dimensional associative k-algebra with identity. There exists a functor $(\bullet \otimes A)^\times$ from the category of commutative k-algebras to the category of groups such that

- to every algebra R, associates the group $(R\otimes A)^\times$ of units of the R-algebra $R \otimes A$, and
- to any morphism f from R to S, associates the unique map from $(R\otimes A)^\times$ to $(S \otimes A)^\times$ such that

$$\begin{tikzcd} (R\otimes A)^\times \arrow[r] \arrow[d] & (S\otimes A)^\times \arrow[d] \\ R\otimes A \arrow[r, "f\otimes \mathrm{id}_A"] & S\otimes A \end{tikzcd}$$

  is commutative, where the columns are the inclusion maps.

Of course, it is a subfunctor of the affine space on A. Also, it turns out that it is even an affine algebraic group over k, which is called the multiplicative group of A. If B is another finite dimensional k-algebra and f is a morphism from

A to B, then there exists a unique natural transformation φ from $(\bullet \otimes A)^\times$ to $(\bullet \otimes B)^\times$, regarded as functors to the category of sets, such that

$$\begin{tikzcd}
(\bullet \otimes A)^\times \arrow[r, "\varphi"] \arrow[d] & (\bullet \otimes B)^\times \arrow[d] \\
\bullet \otimes A \arrow[r] & \bullet \otimes B
\end{tikzcd}$$

is commutative, where the columns are the inclusions and the bottom row is the morphism associated to f, regarded as a linear transformation between k-vector spaces, and we have that is is even a morphism of affine algebraic groups over k. We will refer to it as the morphism associated to f.

Now let V be a finite dimensional k-vector space. Also, let us denote by $(\bullet \otimes \mathrm{End}(V))^\times$ the multiplicative group of $\mathrm{End}(V)$. It turns out that there exists a unique natural transformation from $(\bullet \otimes \mathrm{End}(V))^\times$ to GL_V such that

$$\begin{tikzcd}
(\bullet \otimes \mathrm{End}(V))^\times \arrow[r] \arrow[d] & \mathrm{GL}_V \arrow[d] \\
\bullet \otimes \mathrm{End}(V) \arrow[r] & \mathrm{End}(\bullet \otimes V)
\end{tikzcd}$$

is commutative, where the bottom row is the canonical natural isomorphism and the columns are the inclusions, and it is an isomorphism of algebraic groups. We will refer to it as the canonical isomorphism. Therefore, given a morphism of algebraic groups from $\mathbf{G}$ to $(\bullet \otimes \mathrm{End}(V))^\times$, its composition with the canonical isomorphism from $(\bullet \otimes \mathrm{End}(V))^\times$ to GL_V is a morphism from $\mathbf{G}$ to GL_V, and in this way we obtain a bijection between morphisms from $\mathbf{G}$ to $(\bullet \otimes \mathrm{End}(V))^\times$ and morphisms from $\mathbf{G}$ to GL_V.

1.6 Changing the field of definition

Let K/k be a field extension. If $\mathbf{X}$ is a functor from the category of commutative k-algebras to the category of sets, then there exists a unique functor from the category of commutative K-algebras to the category of sets that

- to every K-algebra R, associates the set that $\mathbf{X}$ associates to R together with its structure of k-algebra obtained from its structure of K-algebra by restriction of scalars through K/k, and that
- to every morphism f of K-algebras, associates the same function as $\mathbf{X}$ does.

It is customary to denote it by $\mathbf{X}_K$, and to refer to it as functor obtained from $\mathbf{X}$ extending scalars through K/k. If $\mathbf{Y}$ is another functor from the category of commutative k-algebras to the category of sets, and ζ is a natural transformation from $\mathbf{X}$ to $\mathbf{Y}$, then there exists a unique natural transformation from $\mathbf{X}_K$ to $\mathbf{Y}_K$ that to any K-algebra R associates the map that is associated to R with its structure of k-algebra by ζ. We will refer to it as the natural transformation obtained from ζ extending scalars through K/k. Of course, if $\mathbf{X}$ is a subfunctor of $\mathbf{Y}$, then $\mathbf{X}_K$ is a subfunctor of $\mathbf{Y}_K$ and the inclusion of $\mathbf{X}_K$ into $\mathbf{Y}_K$ is the map obtain from the inclusion of $\mathbf{X}$ into $\mathbf{Y}$ extending scalars through K/k. In another direction, if $\mathbf{X}$ is an affine algebraic set over k, then $\mathbf{X}_K$ is an affine algebraic set over K. More precisely, if A is a finitely generated k-algebra and η is a natural isomorphism from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{X}$, then $K \otimes A$ together with its canonical structure of K-algebra is finitely generated, and there exists a natural isomorphism from $\mathrm{Hom}(K \otimes A, \bullet)$ to $\mathbf{X}_K$ that to every K-algebra R associates the map given by composition of

$$\mathrm{Hom}(K \otimes A, R) \to \mathrm{Hom}(A, R) \to \mathbf{X}(R),$$

where in the sets in the center and on the right R is meant to be equipped with its structure of k-algebra described above, the map on the left is the canonical bijection, and the map on the right is the one that is associated to R – regarded as a k-algebra – by η. If this is the case, we will refer to $\mathbf{X}_K$ as the affine algebraic set over K obtained from $\mathbf{X}$ extending scalars through K/k. Of course, if also $\mathbf{Y}$ is an affine algebraic set over k – and therefore ζ is a morphism of affine algebraic sets over k – then the natural transformation obtained from ζ extending scalars through K/k is a morphism of affine algebraic sets over K. If this is the case, we will refer to it as the morphism obtained from ζ extending scalars through K/k. Similarly, if $\mathbf{G}$ is a functor from the category of commutative k-algebras to the category of groups, then there exists a unique functor from the category of commutative K-algebras to the category of groups that

- to every K-algebra R, associates the group that $\mathbf{G}$ associates to R together with its structure of k-algebra obtained from its structure of K-algebra by restriction of scalars through K/k, and that
- to every morphism f of K-algebras, associates the same group morphism as $\mathbf{G}$ does.

It is customary to denote it by $\mathbf{G}_K$, and to refer to it as functor obtained from $\mathbf{G}$ extending scalars through K/k. If $\mathbf{H}$ is another functor from the category of commutative k-algebras to the category of groups, and ζ is now a natural transformation from $\mathbf{G}$ to $\mathbf{H}$, then there exists a unique natural transformation from $\mathbf{G}_K$ to $\mathbf{H}_K$ that to any K-algebra R associates the map that is associated to R with its structure of k-algebra by ζ. We will refer to it as the natural transformation obtained from ζ extending scalars through K/k. Regarded as a functor from the category of commutative K-algebras to the category of sets, $\mathbf{G}_K$ is the functor obtained from $\mathbf{G}$, regarded as a functor from the category of commutative k-algebras to the category of sets, extending scalars through K/k. In the same way, regarded as a natural transformation between functors from the category of commutative k-algebras to the category of sets, the natural transformation obtained from ζ, regarded as a natural transformation between functors from the category of commutative k-algebras to the category of sets, extending scalars through K/k. It follows that if $\mathbf{G}$ is an affine algebraic group over k, then $\mathbf{G}_K$ is an affine algebraic group over K. If this is the case, we will refer to it as the affine algebraic group obtained from $\mathbf{G}$ extending scalars through K/k. In addition, if $\mathbf{H}$ is an affine algebraic group over k – hence ζ is a morphism of affine algebraic groups over k – then the natural transformation obtained from ζ extending scalars through K/k is a morphism of affine algebraic groups over K. We will refer to it as the morphism obtained from ζ extending scalars through K/k. Also, if $\mathbf{G}$ is an algebraic subgroup of $\mathbf{H}$, then $\mathbf{G}_K$ is an algebraic subgroup of $\mathbf{H}_K$.

Now let V be a finite dimensional k-vector space. Of course, $K \otimes V$ with its canonical structure of K-vector space is finite dimensional. Also, there exists an isomorphism of affine algebraic groups over K from $\bullet \otimes (K \otimes V)$ to $(\bullet \otimes V)_K$ that to any K-algebra R associates the canonical isomorphism from $R \otimes_K K \otimes_k V$ to $R \otimes_k V$, where in the second tensor product R is meant to be equipped with its structure of k-algebra. Further, there exists an isomorphism from $\mathrm{GL}_{K\otimes V}$ to $(\mathrm{GL}_V)_K$ that to every K-algebra R associates the map sending every automorphism f of $R \otimes_K K \otimes_k V$ to the map given by composition of

$$R \otimes_k V \to R \otimes_K K \otimes_k V \xrightarrow{f} R \otimes_K K \otimes_k V \to R \otimes_k V,$$

where the maps on the left and on the right are the canonical isomorphism between $R \otimes_K K \otimes_k V$ and $R \otimes_k V$.

1.7 Tangent spaces

Let k be a field, $k[\varepsilon]$ a k-algebra generated by an element ε such that $\varepsilon^2 = 0$, and let φ denote the morphism from $k[\varepsilon]$ to k sending ε to 0. If $\mathbf{G}$ is an affine algebraic group over k, its tangent space is the kernel of the group morphism that $\mathbf{G}$ associates to φ. Also, if A is a finitely generated commutative k-algebra, η is a natural isomorphism from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$, and ϵ is the morphism from A to k corresponding through η to the identity of $\mathbf{G}(k)$, then there exists a map from the k-vector space $\mathrm{Der}_\epsilon(A, k)$ of ϵ-derivations of A to k, going to the tangent space of $\mathbf{G}$ and sending any derivation δ to the element of $\mathbf{G}(k[\varepsilon])$ corresponding through η to

$$A \to k[\varepsilon] \qquad a \mapsto \epsilon(a) + \delta(a)\varepsilon,$$

and it is a bijection. Therefore there exists a unique structure of k-vector space on the tangent space of $\mathbf{G}$ such that the previous bijection is an isomorphism of k-vector spaces, and it turns out that it is independent from the choice of A and η. We will refer to it as the standard structure of k-vector space of $\mathbf{G}$. With respect to it, the tangent space is finite dimensional. Also, we will refer to the previous isomorphism as the canonical isomorphism with respect to η. If $\mathbf{H}$ is another affine algebraic group over k and f is a morphism from $\mathbf{G}$ to $\mathbf{H}$, then the map that f associates to $k[\varepsilon]$ sends elements in the tangent space of $\mathbf{G}$ to elements in the tangent space of $\mathbf{H}$. In this way, we obtain a map from the tangent space of $\mathbf{G}$ to the tangent space of $\mathbf{H}$. We will refer to it as the map associated to f. It turns out that it is a linear transformation.

If ψ is a morphism from A to k, a universal ψ-differential of A is a ψ-derivation δ from A to a k-vector space Ω_A such that for any other k-vector space V and any ψ-derivation δ' from A to V there exists a unique linear transformation λ from Ω_A to V such that

$$\begin{tikzcd} A \arrow[r, "\delta"] \arrow[dr, "\delta'"'] & \Omega_A \arrow[d, "\lambda"] \\ & V \end{tikzcd}$$

is commutative. Universal ψ-differentials always exist, and of course they are unique up to isomorphisms. In particular, if A is the symmetric algebra on a finite dimensional k-vector space V, then there exists a unique ψ-derivation from A to V sending any $x \in V$ to itself, and it turns out that it is universal. We refer to it as the canonical universal ψ-differential of A with codomain V. In another direction, if δ is a universal ψ-differential of A with codomain Ω_A, then there exists a function from $\mathrm{Der}_\psi(A, k)$ to the dual Ω_A^* of Ω_A sending any derivation δ' to the unique form λ on Ω_A such that $\delta' = \lambda \circ \delta$, and it is an isomorphism of k-vector spaces. We will refer to it as the canonical isomorphism. In particular, if δ is a universal ϵ-differential of A with codomain Ω_A, then composing the canonical isomorphism from the tangent space of $\mathbf{G}$ to $\mathrm{Der}_\epsilon(A, k)$ with respect to η with the canonical isomorphism from $\mathrm{Der}_\epsilon(A, k)$ to Ω_A^*, we obtain another isomorphism. Again, we will refer to it as the canonical isomorphism.

1.8 Lie algebras and differentials

There are various way to build a functor from the category of affine algebraic groups over $\mathbb{Q}$ to the category of finite dimensional Lie algebras over $\mathbb{Q}$. However, it turns out that these functors are all naturally isomorphic. Then it makes sense to refer to the image of an affine algebraic group $\mathbf{G}$ through one of these functors as the Lie algebra of $\mathbf{G}$. It is customary to denote it by $\mathfrak{g}$. Also, we will use to denote the Lie algebra of $\mathbf{H}$ by $\mathfrak{h}$, and so on. Finally, if φ is a morphism of algebraic groups from $\mathbf{G}$ to $\mathbf{H}$, then we will refer to the associated morphism of Lie algebras from $\mathfrak{g}$ to $\mathfrak{h}$ as the differential of φ, and we will denote it by $\mathrm{d}\varphi$. If $\mathbf{G}$ is connected, then this functorial correspondence has many useful properties. In fact, it turns out that the Lie algebra of the kernel $\mathbf{N}$ of φ is precisely the kernel of $\mathrm{d}\varphi$, and that the differential of the inclusion of $\mathbf{N}$ into $\mathbf{G}$ is the inclusion of $\mathfrak{n}$ into $\mathfrak{g}$. Similarly, the Lie algebra of the image $\mathbf{K}$ of φ is precisely the image of $\mathrm{d}\varphi$, and the differential of the inclusion of $\mathbf{K}$ into $\mathbf{H}$ is the inclusion of $\mathfrak{k}$ into $\mathfrak{h}$. Also, the Lie algebra of the trivial algebraic group is the trivial Lie algebra, and for any finite dimensional $\mathbb{Q}$-vector space V, the Lie algebra of GL_V is $\mathfrak{gl}(V)$. In particular, if $\mathbf{G}$ acts on V, then the differential of the corresponding morphism from $\mathbf{G}$ to GL_V is a morphism of Lie algebras from $\mathfrak{g}$ to $\mathfrak{gl}(V)$, which in turns corresponds to an action of $\mathfrak{g}$ on V. We will refer to it as the differential of the action of $\mathbf{G}$ on V. We have that a vector x in V is fixes under the action of $\mathbf{G}$ if and only if it is fixed under the action of $\mathfrak{g}$. Similarly, a subspace W of V is stable under the action of $\mathbf{G}$ if and only if it is under the action of $\mathfrak{g}$. If this is the case, the differentials of the induced actions of $\mathbf{G}$ on W and on V/W are the induced actions of $\mathfrak{g}$ on W and on V/W. If $\mathbf{G}$ also acts on V', then the differential of the action of $\mathbf{G}$ on $V \oplus V'$ is the direct sum of the action of $\mathfrak{g}$ on V and on V' given by the differentials of the actions of $\mathbf{G}$ on V and on V'.

Now let $\mathbf{G}$ be a connected affine algebraic group over $\mathbb{Q}$, A be a finitely generated $\mathbb{Q}$-algebra, η a natural isomorphism from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$, and ι a monomorphism from $\mathbf{G}$ to some GL_V. Also, let us denote by S the symmetric algebra on the dual of $\mathrm{End}(V)$. By Yoneda lemma there exists a unique morphism of algebras φ from S to A such that

$$\begin{tikzcd}
\mathrm{Hom}(A,\bullet) \arrow[r, "\sharp\circ\varphi"] \arrow[d, "\eta"] & \mathrm{Hom}(S,\bullet) \arrow[d] \\
\mathbf{G} \arrow[r] & \mathrm{End}(\bullet\otimes V)
\end{tikzcd}$$

is commutative, where the bottom row is the composition of ι with the inclusion of GL_V into $\mathrm{End}(\bullet \otimes V)$, and the right column is the canonical natural isomorphism. Let $f_1, \ldots, f_n$ be a finite set of generators for the kernel of φ, and let $x_1, \ldots, x_m$ be a basis for V. Also, let us denote by $\mathbb{Q}[\hat{X}]$ the polynomial algebra with rational coefficients in the indeterminates X_{ij}, where i and j are between 1 and m. Then the isomorphism from S to $\mathbb{Q}[\hat{X}]$ with respect to $x_1, \ldots, x_m$ sends $f_1, \ldots, f_n$ to polynomials in $\mathbb{Q}[\hat{X}]$. Let us denote by $\mathrm{d}f_1, \ldots, \mathrm{d}f_n$ their differentials. Since their are homogeneous polynomials of degree one, their images through the isomorphism between $\mathbb{Q}[\hat{X}]$ and S are in $\mathrm{End}(V)^*$, and it makes sense to consider their orthogonal space $\mathfrak{g}$, which is of course a subspace of $\mathrm{End}(V)$. It turns out that it is the unique sub-Lie-algebra of $\mathfrak{gl}(V)$ such that $\mathfrak{g}$ is the Lie algebra of $\mathbf{G}$ and that the inclusion of $\mathfrak{g}$ into $\mathfrak{gl}(V)$ is the differential of ι. In particular, in this setting it is easy to compute the subspace W of V consisting of the vectors fixed under the action of $\mathbf{G}$ on V corresponding to ι. In fact, if $x_1, \ldots, x_m$ is any set of endomorphisms of V forming a basis of $\mathfrak{g}$, then W is the intersection of the kernels of the x_i.

1.9 Unipotent affine algebraic groups over $\mathbb{Q}$

An affine algebraic group $\mathbf{G}$ over $\mathbb{Q}$ is unipotent if every non-zero linear representation admits a non-zero fixed vector. If this is the case, $\mathbf{G}$ is connected. Also, any linear representation of $\mathbf{G}$ on a finite dimensional vector space V admits a flag, that is to say, a chain

$$0 = V_0 \leq \cdots \leq V_i \leq \cdots \leq V_m = V$$

of subspaces of V which are $\mathbf{G}$-stable and such that the vectors in the $\frac{V_{i+1}}{V_i}$ are fixed under the action of $\mathbf{G}$ on the $\frac{V}{V_i}$. The integer m is called the length of the flag. Otherwise stated, the image of any morphism of algebraic groups from $\mathbf{G}$ to GL_V consists of unipotent automorphisms.

Of course it makes sense to consider the full subcategory of the category of the affine algebraic groups over $\mathbb{Q}$ whose objects are just the unipotent algebraic groups. We will refer to it as the category of unipotent affine algebraic groups over $\mathbb{Q}$. It is not hard to see that it is closed under subobjects and quotient objects. In a similar way, we have at hand the category of the nilpotent finite dimensional Lie algebras over $\mathbb{Q}$, that is to say, the full subcategory of the category of the finite dimensional Lie algebras over $\mathbb{Q}$ whose objects are the nilpotent Lie algebras. Again, it is closed under subobjects and quotient objects. Also, if an affine algebraic group over $\mathbb{Q}$ is unipotent, then its Lie algebra is nilpotent. Therefore we have at hand a functor from the category of unipotent affine algebraic groups over $\mathbb{Q}$ to the category of nilpotent finite dimensional Lie algebras over $\mathbb{Q}$, sending any algebraic group to its Lie algebras and any morphism to its differential. It turns out that it is an equivalence between the two categories. As a functor from nilpotent finite dimensional Lie algebras over $\mathbb{Q}$ to affine algebraic sets over $\mathbb{Q}$, a quasi-inverse sends any Lie algebra $\mathfrak{g}$ to the algebraic set $\bullet \otimes \mathfrak{g}$ corresponding to $\mathfrak{g}$ – regarded as a finite dimensional vector space over $\mathbb{Q}$ – and acts in the obvious way on the morphisms. Also, if $\mathbf{G}$ is a unipotent algebraic subgroup of some GL_V and $\mathfrak{g}$ is the unique sub-Lie-algebra of $\mathfrak{gl}(V)$ such that $\mathfrak{g}$ is the Lie algebra of $\mathbf{G}$ and the inclusion of $\mathfrak{g}$ into $\mathfrak{gl}(V)$ is the differential on the inclusion of $\mathbf{G}$ into GL_V, then $\mathfrak{g}$ consists of nilpotent endomorphisms, and the natural isomorphism from $\mathbf{G}$ to $\bullet\otimes\mathfrak{g}$ sends any rational point g of $\mathbf{G}$ to its logarithm, that is to say, to

$$\sum_{i=1}^{\infty}(-1)^{i-1}\ \frac{1}{i!}\ (g-\mathrm{id}_V)^i\ ,$$

while its inverse sends any element x of $\mathfrak{g}$ to its exponential, that is to say, to

$$\sum_{i=0}^{\infty}\frac{1}{i!}x^i.$$

Of course the functions are well-defined since both sums have only finitely many non-zero terms. Usually, we will denote the logarithm of g by $\log(g)$, and the exponential of x by $\exp(x)$. As a corollary of the previous results, note that if $\mathbf{G}$ and $\mathbf{Q}$ are both unipotent affine algebraic groups over $\mathbb{Q}$, then the image of the rational points of $\mathbf{G}$ through any epimorphism of algebraic groups from $\mathbf{G}$ to $\mathbf{Q}$ is the whole group of the rational points of $\mathbf{Q}$.

1.10 Groups of multiplicative type

Let k be a perfect field. We say that a linear representation of an affine algebraic group $\mathbf{G}$ over k on a finite dimensional k-vector space V is diagonalizable if V is the sum of its one dimensional $\mathbf{G}$-stable subspaces, and that $\mathbf{G}$ is diagonalizable if every linear representation of $\mathbf{G}$ on the finite dimensional k-vector spaces is. We will refer to the full subcategory of the category of affine algebraic groups over k whose objects are the diagonalizable groups as the category of the diagonalizable affine algebraic groups over k. We have that it is closed under subobjects and quotient objects. Also, if M is a finitely generated abelian group, then there exists a unique affine algebraic group $\mathrm{Hom}(M, \bullet^\times)$ over k that

- to every algebra R, associates the group $\mathrm{Hom}(M, R^\times)$ of the group morphisms from M to the group of units $R^\times$ of R, and that
- to every morphism f from R to S, associates

$$\mathrm{Hom}(M, R^\times) \to \mathrm{Hom}(M, S^\times) \qquad g \mapsto f\circ g.$$

We have that $\mathrm{Hom}(M, \bullet^\times)$ is a diagonalizable affine algebraic group. Further, if N is another finitely generated abelian group and φ is a morphism from M to N, then there exists a morphism $\sharp\circ\varphi$ from $\mathrm{Hom}(N, \bullet^\times)$ to $\mathrm{Hom}(M, \bullet^\times)$ sending any algebra R to

$$\mathrm{Hom}(N, R^\times) \to \mathrm{Hom}(M, R^\times) \qquad \psi \mapsto \psi\circ\varphi.$$

Finally, there exists a contravariant functor from the category of finitely generated abelian groups to the category of diagonalizable affine algebraic groups over k such that

- sends any abelian group M to $\mathrm{Hom}(M, \bullet^\times)$, and that
- sends any morphism φ from M to N to $\sharp \circ \varphi$,

and we have that it is an anti-equivalence of categories.

Now let $\overline{k}$ be an algebraic closure of k. We say that an affine algebraic group $\mathbf{G}$ over k is of multiplicative type if $\mathbf{G}_{\overline{k}}$ is diagonalizable. The full subcategory of the affine algebraic groups over k whose objects are the groups of multiplicative type is closed under subobjects and quotient objects. Also, let us denote by Γ the Galois group of $\overline{k}/k$. A Γ-module M is affine if it is finitely generated as an abelian group, and if there exists a finite Galois extension F of k contained in $\overline{k}$ such that the kernel of the action of Γ on M is contained in the kernel of the canonical epimorphism from Γ to the Galois group of F/k. If this is the case, then F is called a field of definition for M. We will refer to the full subcategory of the Γ-modules whose objects are the affine Γ-modules as the category of affine Γ-modules. Again, it is closed under subobjects and quotient objects. If R is a commutative k-algebra, then there exists a unique action of Γ on the group $(R \otimes \overline{k})^\times$ of units of $R \otimes \overline{k}$ such that the product of $\gamma \in \Gamma$ and of $x \otimes \alpha \in (R \otimes \overline{k})^\times$ is $x \otimes \gamma(\alpha)$. We will refer to it as the standard structure of Γ-module on $(R \otimes \overline{k})^\times$. If M is an affine Γ-module, then there exists an affine algebraic group $\mathrm{Hom}(M, (\bullet \otimes \overline{k})^\times)$ over k such that

- sends every algebra R to the group $\mathrm{Hom}(M, (R \otimes \overline{k})^\times)$ of morphisms of Γ-modules from M to $(R \otimes \overline{k})^\times$ together with its standard structure of Γ-module, and that
- sends every morphism f from R to S to
$$\mathrm{Hom}(M, (R \otimes \overline{k})^\times) \to \mathrm{Hom}(M, (S \otimes \overline{k})^\times) \qquad g \mapsto \overline{f} \circ g,$$
where $\overline{f}$ is obtained from f extending scalars to $\overline{k}$.

If φ is a morphism from M to another Γ-module N, then there exists a morphism $\sharp \circ \varphi$ from $\mathrm{Hom}(N, (\bullet \otimes \overline{k})^\times)$ to $\mathrm{Hom}(M, (\bullet \otimes \overline{k})^\times)$ that to any algebra R associates
$$\mathrm{Hom}(N, (R \otimes \overline{k})^\times) \to \mathrm{Hom}(M, (R \otimes \overline{k})^\times) \qquad \psi \mapsto \psi \circ \varphi.$$

Further, there exists a contravariant functor from the category of affine Γ-modules to the category of affine algebraic groups over k of multiplicative type that

- to any module M associates $\mathrm{Hom}(M, (\bullet \otimes \overline{k})^\times)$, and that
- to any morphism f associates $\sharp \circ f$,

and we have that it is an anti-equivalence of categories. Also, we say that an affine algebraic group $\mathbf{G}$ over k is a torus if it is isomorphic to $\mathrm{Hom}(M, (\bullet \otimes \overline{k})^\times)$ for some torsion-free Γ-module M. If k has characteristic 0, then a group of multiplicative type is a torus if and only if it is connected. In another direction, let M be an affine Γ-module, F a field of definition for M, R a $\overline{k}$-algebra, and let us denote by G the Galois group of F/k. Also, let R^G denote the cartesian product of copies of R indexed by elements in G, together with its standard structure of ring and with the structure of F-algebra given by

$$\alpha(x_g)_g = (g(\alpha)x_g)_g$$

for every $\alpha \in F$ and $(x_g)_g$ in the cartesian product of $|G|$ copies of R. Then

$$G \times (R^G)^\times \to (R^G)^\times \qquad (\hat{g}, (x_g)_g) \mapsto (x_{g\hat{g}})_g$$

is an action, and in this way

$$\varphi : (R \otimes F)^\times \to (R^G)^\times \qquad x \otimes \alpha \mapsto (g(\alpha)x)_g$$

is an isomorphism of G-modules, with respect to the standard structure of G-module of $(R \otimes F)^\times$. Also, there exists a morphism from $\mathrm{Hom}(M, R^\times)$ to the group $\mathrm{Hom}_G(M, (R^G)^\times)$ of morphisms of G-modules from M to $(R^G)^\times$, sending f to the map which in turn sends any x to $(f(gx))_g$. Composing it with

$$\mathrm{Hom}_G(M, (R^G)^\times) \to \mathrm{Hom}_G(M, (R \otimes F)^\times) \qquad f \mapsto \varphi^{-1} \circ f,$$

we obtain an isomorphism from $\mathrm{Hom}(M, R^\times)$ to $\mathrm{Hom}_G(M, (R \otimes F))^\times$. It turns out that the set of these maps over the $\overline{k}$-algebras is even an isomorphism of affine algebraic groups over $\overline{k}$ between $\mathrm{Hom}(M, (\bullet \otimes \overline{k})^\times)_{\overline{k}}$ and $\mathrm{Hom}(M, \bullet^\times)$. We will refer to it as the canonical isomorphism. If N is another affine Γ-module, and f is a morphism from N to M, then

$$\begin{tikzcd}
\mathrm{Hom}(M, (\bullet \otimes \overline{k})^\times)_{\overline{k}} \arrow[r] \arrow[d] & \mathrm{Hom}(N, (\bullet \otimes \overline{k})^\times)_{\overline{k}} \arrow[d] \\
\mathrm{Hom}(M, \bullet^\times) \arrow[r, "\sharp \circ f"] & \mathrm{Hom}(N, \bullet^\times)
\end{tikzcd}$$

is commutative, where the columns are the canonical isomorphisms and the top row is the map obtained from $\sharp \circ f$ extending scalars to $\overline{k}$.

Now let D be a finite dimensional commutative and semisimple k-algebra, let us denote by X the set of morphisms from D to $\overline{k}$, and by $\mathbb{Z}[X]$ the free abelian group with basis X. Then there exists a unique action of Γ on $\mathbb{Z}[X]$ such that the product of $\gamma \in \Gamma$ and of $x \in X$ is the morphism from D to $\overline{k}$ given by composition of x and γ. We refer to it as the standard structure of Γ-module on $\mathbb{Z}[X]$. If F is the splitting field of D into $\overline{k}$, then we have that the kernel of the action of Γ on $\mathbb{Z}[X]$ is contained in the kernel of the canonical projection of Γ onto the Galois group G of F/k. Therefore on one hand we obtain that $\mathbb{Z}[X]$ is a torsion-free affine Γ-module, and on the other hand we have that $\mathbb{Z}[X]$ is endowed with a structure of G-module. We refer to it as the standard structure of G-module on $\mathbb{Z}[X]$. Also, there exists an isomorphism from $(\bullet \otimes D)^\times$ to $\mathrm{Hom}(\mathbb{Z}[X], (\bullet \otimes \overline{k})^\times)$ that to any algebra R associates the map that sends any unit u of $R \otimes D$ to

$$\mathbb{Z}[X] \to (R \otimes \overline{k})^\times \qquad x \mapsto \overline{x}(u),$$

where $\overline{x}$ is the map obtained from x extending scalars to R. We refer to it as the canonical isomorphism. In particular, it follows that $(\bullet \otimes D)^\times$ is a torus.

Further, there exists a unique isomorphism of affine algebraic groups ζ over $\overline{k}$ from $\mathrm{Hom}(\mathbb{Z}[X], \bullet^\times)$ to $(\bullet \otimes \overline{k} \otimes D)^\times$ such that

$$\begin{tikzcd}
\mathrm{Hom}(\mathbb{Z}[X], (\bullet \otimes \overline{k})^\times)_{\overline{k}} \arrow[r] \arrow[d] & (\bullet \otimes D)^\times_{\overline{k}} \arrow[d] \\
\mathrm{Hom}(\mathbb{Z}[X], \bullet^\times) \arrow[r, "\zeta"] & (\bullet \otimes \overline{k} \otimes D)^\times
\end{tikzcd}$$

is commutative, where the top row is the isomorphism obtained from the canonical isomorphism between $\mathrm{Hom}(\mathbb{Z}[X], (\bullet \otimes \overline{k})^\times)$ and $(\bullet \otimes D)^\times$ extending scalars to $\overline{k}$ and the columns are the canonical isomorphisms. Once again, we will refer to it as the canonical isomorphism.

1.11 Vector spaces and lattices

Let V be a finite dimensional $\mathbb{Q}$-vector space. A lattice L in V is a finitely generated subgroup of V. Of course L is in particular a torsion-free abelian group, and its rank is less or equal to the dimension of V. In particular, every lattice admits a basis. Clearly, any basis of L consists of linearly independent vectors of V. Also, L is called full-dimensional if the subspace generated by L is the whole V, or, equivalently, if the rank of L is equal to the dimension of V. If this is the case, then a basis for L is also a basis for V. If W is a subspace of V, then $L \cap W$ is a lattice in W, $L + W/W$ is a lattice in V/W, and they are full-dimensional as soon as L is.

Now let W and W' be two subspaces of V, V' another finite dimensional $\mathbb{Q}$-vector space, f a linear transformation from V to V', L and N two lattices in V such that $N \leq L$ and L/N is torsion-free, and L' a lattice in V'. There exist well known algorithms to perform very basic but extremely useful computations with these objects. For instance, it is rather straightforward to compute the intersection $W \cap W'$ of W and W', the quotient V/W of V on W, the direct sum $V \oplus V'$ of V and V', the orthogonal $W^\perp$ of W with respect to the canonical bilinear form between V and its dual, as well as the kernel and the image of f, and the anti-images of any element of V' through f. Here the main tool is Gaussian elimination. Also, it is easy to compute $L \oplus L'$. Instead, computing $L \cap W$, $L + W/W$, a complement to N in L and to test membership of an element of V to $L + W$ are a bit harder problems. Since $W \cap L$ is the kernel of the group morphism given by composition of

$$L \to V \to \frac{V}{W} \ ,$$

where the letf arrow is the inclusion and the right arrow is the canonical projection, computing $W \cap L$ reduces to the problem of finding all the solutions with integer coefficients of $Ax = 0$, where A is a $m \times n$ matrix with rational coefficients, whose columns are the coordinates with respect to some basis of V/W of the images of a basis for L through the map above. It is well-known that there exist $S \in \mathrm{M}_{m \times n}(\mathbb{Q})$ whose entries outside the main diagonal are 0, $Q \in \mathrm{GL}_n(\mathbb{Z})$, and $P \in \mathrm{GL}_m(\mathbb{Q})$ such that $S = PAQ$, and they can be computed quite easily. This is very useful, since the elements we are searching for are all and only the Qy, where y ranges over the solutions of $Sy = 0$, which in turn are very easy to compute. With similar techniques, it is possible to perform all the other considered task, too. Also, if we are given $x \in V$ which is contained in $L + W$, it is possible to compute $y \in L$ and $x' \in L$ whose sum is x. Finally, let $x_1, \ldots, x_m$ be elements of V. Then we are even able to compute the kernel K of

$$\mathbb{Z}^m \to \frac{V}{L+W}$$

which sends the i-th element of the canonical basis of $\mathbb{Z}^m$ to x_i for every i between 1 and m. Indeed, let $y_1, \ldots, y_n$ be a basis of L. Then K is the image through

$$\mathbb{Z}^{m+n} \to \mathbb{Z}^m \quad , \quad (a_1, \ldots, a_m, b_1, \ldots, b_n) \mapsto (a_1, \ldots, a_m)$$

of the kernel of

$$\mathbb{Z}^{m+n} \to \frac{V}{W}$$

which for every i between 1 and m sends the i-th element of the canonical basis of $\mathbb{Z}^{m+n}$ to x_i, and for any i between 1 and n sends the $i+m$-th element of the canonical basis to y_i. A treatment of this kind of problems can be found for example [Si].

1.12 T-groups

A T-group is a finitely generated, torsion-free nilpotent group. Of course examples of T-groups are the finitely generated torsion-free abelian groups, while any T-group is in particular a polycyclic group. In particular, the Hirsch length is an invariant of any T-group. Also, subgroups of T-groups are again T-groups, and if a group G has a central subgroup N such that both N and G/N are T-groups, then also G is.

It is well-known that a group G is a T-group if and only if it admits a central series with infinite cyclic factors. We will call such a series a T-series. Of course, the length of any T-series is an invariant for G, being equal to its Hirsch length. Also, if G is not trivial, then we will say that a finite set of generators $g_1, \ldots, g_m$ for G is a T-sequence if and only if the chain of subgroups

$$G = G_1 \geq \cdots \geq G_i \geq \cdots \geq G_{m+1} = 1,$$

where for any i between 1 and m we put

$$G_i = \langle g_i, \ldots, g_m \rangle,$$

is a T-series for G. Of course, any basis of a finitely generated torsion-free abelian group is also a T-sequence. Also, any T-sequence for a T-group is in particular a polycyclic sequence for it. It will be convenient to extend this terminology saying that the empty set is a T-sequence for the trivial group. For a general discussion about T-groups, and more generally about finitely generated nilpotent groups, see for example [Ro].

1.13 Semisimple algebras, fields, and orders

Let k be a perfect field, and D a finite dimensional k-algebra. If V is a finite dimensional k-vector space and α is a left action of D on V, then there exists a morphism ρ from D to $\mathrm{End}(V)$ with its standard structure of k-algebra that to any a associates the endomorphism of V sending any x to $\alpha(a,x)$, and in this way we obtain a bijection between the set of left actions of D on V and the set of morphisms from D to $\mathrm{End}(V)$. In the special case in which D is a subalgebra of $\mathrm{End}(V)$, we will refer to the left action of D on V corresponding to the inclusion of D into $\mathrm{End}(V)$ as the natural action of D. If E is another finite dimensional k-algebra and f is a morphism from D to E, then there exists a unique action of D on the undelying k-vector space of E sending (a,b) to the product of $f(a)$ and b in E. We will refer to it as the action induced by f. In the special case in which E is actually D and f is the identity function of D, we will also refer to it as the regular action of D. Of course, f is a morphism of D-modules with respect to the regular action of D on itself and the action of D on E induced by f. Further, we say that an action of D on V is diagonalizable if V is the sum of its one-dimensional stable subspaces. If this is the case, then the action of D on $\mathrm{End}(V)$ induced by the morphism from D to $\mathrm{End}(V)$ which in turn corresponds to the action of D on V, is diagonalizable, too. If in addition W is another finite dimensional k-vector space on which D acts in such a way that there exists an injective morphism of D-modules from W to V, then also the action of D on W is diagonalizable. Further, we say that D is diagonalizable if the regular action is.

Now let K/k be a field extension. If V is a finite dimensional k-vector space and α is an action of D on V, then the bilinear map obtained from α extending scalars to K is an action of $K \otimes D$ with its standard structure of K-algebra on $K \otimes V$. Let us denote by ϱ the morphism from $K \otimes D$ to $\mathrm{End}(K \otimes V)$ corresponding to it. Also, let us denote by ρ the morphism from $K \otimes D$ to $K \otimes \mathrm{End}(V)$ obtained from the morphism from D to $\mathrm{End}(V)$ which in turn corresponds to α, extending scalars to K. Then

$$\begin{tikzcd} K \otimes D \arrow[r, "\varrho"] \arrow[dr, "\rho"] & \mathrm{End}(K \otimes V) \arrow[d] \\ & K \otimes \mathrm{End}(V) \end{tikzcd}$$

is commutative, where the vertical arrow is the canonical isomorphism. In particular, the canonical isomorphism between $\mathrm{End}(K \otimes V)$ and $K \otimes \mathrm{End}(V)$ is a morphism of $(K \otimes D)$-modules.

Now let D be commutative. We say that D is semisimple if $\overline{k} \otimes D$ is diagonalizable. A typical example are the finite field extensions of k. If this is the case, there exist simple ideals $E_1, \dots, E_m$ of D whose internal sum is direct and is equal to the whole D. Also, they are unique with respect to these properties, and they are called the decomposition of D is simple ideals. Further,

$$\varphi : E_1 \times \cdots \times E_m \to D \qquad (a_1, \dots, a_m) \mapsto a_1 + \cdots + a_m$$

is a k-algebra isomorphism with respect to the standard structure of k-algebra on the cartesian product of the E_i. We will refer to it as the canonical isomorphism.

For every i between 1 and m, let e_i be the unique element of E_i such that $e_1+\cdots+e_m$ is the identity of D. We will refer to $e_1,\ldots,e_m$ as the decomposition of the identity associated to $E_1,\ldots,E_m$. It turns out that

$$e_i^2 = e_i \quad \text{and} \quad e_ie_j = 0$$

for every i and j between 1 and m, and $i \neq j$. Also, the E_i are fields, whose identities are the e_i. Further, if D acts on a finite dimensional k-vector space V, then V is the direct sum of the images V_i of V through e_i, for i between 1 and m, and there exists a unique function from the cartesian product of E_i and V_i to V_i such that

$$\begin{tikzcd} E_i \times V_i \arrow[r] \arrow[d] & V_i \arrow[d] \\ D \times V \arrow[r] & V \end{tikzcd}$$

is commutative, where the bottow row is the action of D on V and the colums are the inclusions. It is an action of E_i on V_i, which is called the induced action, and it is faithful as soon as the action of D on V is. Therefore

$$E_1 \times \cdots \times E_m \ \times \ V_1 \oplus \cdots \oplus V_m \to V_1 \oplus \cdots \oplus V_m$$

given by

$$((a_1,\ldots,a_m),(x_1,\ldots,x_m)) \mapsto (a_1.x_1,\ldots,a_m.x_m),$$

where of course $a_i.x_i$ denotes the image of (a_i,x_i) through the action of E_i on V_i, is an action of $E_1 \times \cdots \times E_m$ on $V_1 \oplus \cdots \oplus V_m$ such that

$$\begin{tikzcd} \prod_{i=1}^m E_i \ \times \ \oplus_{i=1}^m V_i \arrow[r] \arrow[d, "\varphi\times\iota"'] & \oplus_{i=1}^m V_i \arrow[d, "\iota"] \\ D \times V \arrow[r] & V \end{tikzcd}$$

where ι is the canonical isomorphism from $V_1 \oplus \cdots \oplus V_m$ to V. A standard reference for these facts is [DKD]. Also, there exist algorithms to compute $E_1,\ldots,E_m$ given D, as well as to compute $e_1,\ldots,e_m$. See for example [EG].

Now let E be a number field, that is to say, a finite dimensional $\mathbb{Q}$-algebra which is also a field. It is easy to see that the torsion subgroup of the group of units of the ring of integers $\mathcal{O}_E$ of E is cyclic. Also, Dirichlet unit theorem asserts that the torsion-free rank of the group of units of $\mathcal{O}_E$ is equal to $\frac{1}{2}(n+r)-1$, where r is the number of morphisms of E into $\mathbb{R}$ and n is the number of morphisms of E into $\mathbb{C}$. In particular, the group of units of $\mathcal{O}_E$ is finitely generated. An order $\mathcal{O}$ of E is a subring of the ring of integers of E which is also a full-dimensional lattice of E, once we regard it as a $\mathbb{Q}$-vector space. Of course, its group of units is finitely generated, too. In [PZ], Pohst and Zassenhaus provide an algorithm that, given a number field together with an order of its, computes a finite set of generators for the group of units of the order. Finally, let $\alpha_1,\ldots,\alpha_m$ be non-zero algebraic integers of E. Then there exists a unique group morphism from $\mathbb{Z}^m$ to $E^\times$ that for every i between 1 and m sends the i-th element of the canonical basis of $\mathbb{Z}^m$ to α_i. Of course its kernel is finitely generated. In [Ge], Ge provided an algorithm to compute a finite set of generators for it.

1.14 Orbits and stabilizers

Let G be a group acting on the left on a set Ω. Also, let N be a normal subgroup of G, and ω an element in Ω. Let us denote by Ω/N the orbit space of Ω under the action of N on Ω coming from the action of G on Ω by restriction. Since N is normal in G, there exists a unique left action of G on Ω/N such that the canonical projection of Ω on Ω/N is a morphism of G-sets, and it is easy to check that N is contained in the stabilizer $G_{N\omega}$ of $N\omega$ with respect to this action. Now let T be a transversal for $G_{N\omega}$ in G, and

$$S = \{g_\lambda \mid \lambda \in \Lambda\} \quad \text{for some set } \Lambda$$

a subset of G such that $G_{N\omega}$ is generated by the union of S and N. Then for every g_λ in S there exists $n \in N$ such that $g_\lambda\omega = n\omega$. For every g_λ, let us choose a n_λ in N with such a property, and let us put $\widehat{g}_\lambda = g_\lambda n_\lambda^{-1}$. Then it can be shown that

$$G\omega = \bigcup_{\tau\in T} \tau N\omega$$

and that

$$G_\omega = HN_\omega,$$

where H is the subgroup of G generated by the $\widehat{g}_\lambda$ for $\lambda \in \Lambda$.

Now let us suppose that G is a finitely generated abelian group, that $g_1, \ldots, g_m$ form a finite set of generators for it, and that the orbit of ω under G is finite. If H is any subgroup of G, we will say that a finite subset $\mathcal{O}$ of Ω, a finite subset X of G and a map β from $\mathcal{O}$ to H are a solution of the finite orbit and stabilizer problem for H and ω if $\mathcal{O}$ is the orbit of ω under the action of H on Ω given by restriction of the action of G on it, X is a finite set of generators for H_ω, and

$$\omega' = \beta(\omega')\omega$$

for every ω' in $\mathcal{O}$. Also, for every i between 1 and m, put

$$G_i = \langle g_i, \ldots, g_m \rangle.$$

Of course, $\mathcal{O}^{(m+1)} = \{\omega\}$, $X^{(m+1)} = \emptyset$ and

$$\beta^{(m+1)} : \mathcal{O}^{(m+1)} \to G_{m+1} \qquad \omega \mapsto 1$$

are a solution of the finite orbit and stabilizer problem for G_{m+1} and ω. Now let i be an integer between 1 and m, and let us suppose that $\mathcal{O}^{(i+1)}$, $X^{(i+1)}$ and β^{i+1} are a solution of the finite orbit and stabilizer problem for G_{i+1} and ω. Also, let l be the minimum positive integer l such that

$$g_i^{l+1}\mathcal{O}^{(i+1)} = \mathcal{O}^{(i+1)}.$$

Of course it surely exists since the orbit of ω is finite. Also, let us put

$$\mathcal{O}^{(i)} = \bigcup_{i=1}^{l} g_i^j \mathcal{O}^{i+1}$$

and

$$X^{(i)} = X^{(i+1)} \cup \{\widehat{g}_i\},$$

where

$$\widehat{g}_i = g_i^{l+1}\ [\beta^{(i+1)}(g_i^{l+1}\omega)]^{-1},$$

and let $\beta^{(i)}$ be the map from $\mathcal{O}^{(i)}$ to $G^{(i)}$ given by

$$g_i^j\ \omega' \mapsto g_i^j\ \beta^{(i+1)}(\omega')$$

for every ω' in $\mathcal{O}^{(i+1)}$ and every j between 0 and l. Also, let us denote by K the stabilizer of $G_{i+1}\omega$ with respect to the action of G_i on Ω/G_{i+1}. Then

$$\{1, g_i, \ldots, g_i^l\}$$

is a transversal for K in G_i, K is generated by G_{i+1} and g_i^{l+1}, and

$$g_i^{l+1}\omega = \beta^{(i+1)}(g_i^{l+1}\omega)\ \omega.$$

Therefore by the previous results we have that $\mathcal{O}^{(i)}$, $X^{(i)}$ and $\beta^{(i)}$ are a solution of the finite orbit and stabilizer problem for G_i and ω. Since $G_1 = G$, this discussion gives an algorithm for computing a finite set of generators for G_ω, which is usually called the finite orbit stabilizer algorithm. For information about it can be found in [Ei].

Chapter 2

The problem

In this chapter we introduce the main problem we will deal with in the next chapters. In the first two sections, we give the notions of algebraic matrix group and of arithmetic group, as well as an historical account of some results concerning them. Finally, in the last two sections we will give a precise definition of the problem, and we will justify our interest in it.

2.1 Algebraic matrix groups

Let m be an integer greater than 1. Also, let us denote by $\hat{X}$ the set of indeterminates X_{ij} where i and j are integers between 1 and m, and by $\mathbb{C}[\hat{X}]$ the polynomial algebra with complex coefficients in the indeterminates in $\hat{X}$. If

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \in \mathrm{GL}_m(\mathbb{C}),$$

then there exists a unique morphism of $\mathbb{C}$-algebras from $\mathbb{C}[\hat{X}]$ to $\mathbb{C}$ sending any X_{ij} in $\hat{X}$ to a_{ij}. If f is a polynomial in $\mathbb{C}[\hat{X}]$, we denote by $f(A)$ its image through such a morphism. Also, we denote by $V(f)$ the set of elements A in $\mathrm{GL}_m(\mathbb{C})$ such that $f(A) = 0$. Further, given a finite set $f_1, \ldots, f_n$ of polynomials in $\mathbb{C}[\hat{X}]$, we denote by $V(f_1, \ldots, f_n)$ the intersection of the $V(f_i)$ for all the f_i between f_1 and f_n.

Given a subgroup G of $\mathrm{GL}_m(\mathbb{C})$, we say that G is an algebraic matrix subgroup of $\mathrm{GL}_m(\mathbb{C})$, or, more briefly, an algebraic matrix group, if there exists a finite set of polynomials $f_1, \ldots, f_n$ such that

$$G = V(f_1, \ldots, f_n).$$

If this is the case, we say that $f_1, \ldots, f_n$ define G. Of course, such polynomials are in general not unique. If they can be taken with rational coefficients, then we say that G is defined over $\mathbb{Q}$.

Now let us denote by GL_m the general linear group of order m over $\mathbb{Q}$. It turns out that, if $\mathbf{G}$ is an algebraic subgroup of GL_m, then $\mathbf{G}(\mathbb{C})$ is an algebraic matrix subgroup of $\mathrm{GL}_m(\mathbb{C})$ defined over $\mathbb{Q}$. More precisely, let us denote by $\mathbb{Q}[\hat{X}]$ the polynomial algebra with rational coefficients in the set of indeterminates $\hat{X}$. Also, let us put

$$\det = \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) X_{1\sigma(1)} \cdots X_{m\sigma(m)},$$

where S_m is the symmetric group on $\{1, \ldots, m\}$ and sgn is the sign morphism, and let us denote by $\mathbb{Q}[\hat{X}]_{\det}$ the localization of $\mathbb{Q}[\hat{X}]$ at det. By hypothesis there exist a finitely generated $\mathbb{Q}$-algebra A together with a natural isomorphism η from $\operatorname{Hom}(A, \bullet)$. Further, by Yoneda lemma there exists a unique morphism π from $\mathbb{Q}[\hat{X}]_{\det}$ to A such that

$$\begin{tikzcd}
\operatorname{Hom}(A, \bullet) \arrow[r, "\sharp\circ\pi"] \arrow[d, "\eta"] & \operatorname{Hom}(\mathbb{Q}[\hat{X}]_{\det}, \bullet) \arrow[d, "\simeq"] \\
\mathrm{G} \arrow[r] & \mathrm{GL}_m
\end{tikzcd}$$

is commutative, where the bottom row is the inclusion and the right column is the canonical isomorphism. Also, let us denote by $\mathfrak{i}$ the kernel of the map given by composition of

$$\mathbb{Q}[\hat{X}] \to \mathbb{Q}[\hat{X}]_{\det} \xrightarrow{\pi} A,$$

where the left arrow is the localization map. Then $\mathfrak{i}$ is a radical ideal, and $\mathbf{G}(\mathbb{C})$ is defined by any finite set $f_1, \ldots, f_n$ of polynomials in $\mathbb{Q}[\hat{X}]$ such that

$$\mathfrak{i} = \sqrt{(f_1, \ldots, f_n)}.$$

Also, the map that associates to any $\mathbf{G}$ its group of complex points is a bijection from the set of algebraic subgroups of GL_m to the set of algebraic matrix subgroups of $\mathrm{GL}_m(\mathbb{C})$ defined over $\mathbb{Q}$. These facts are a direct consequence of Proposition 11.1 and of Theorem 2.31 of [Mi2].

2.2 Some old results

Let G be an algebraic matrix subgroup of some $\mathrm{GL}_m(\mathbb{C})$ defined over $\mathbb{Q}$, and put

$$G_{\mathbb{Q}} = G \cap \mathrm{GL}_m(\mathbb{Q}) \quad \text{and} \quad G_{\mathbb{Z}} = G \cap \mathrm{GL}_m(\mathbb{Z}).$$

A subgroup Γ of $G_{\mathbb{Q}}$ is an arithmetic subgroup of G if $\Gamma \cap G_{\mathbb{Z}}$ has finite index in both Γ and $G_{\mathbb{Q}}$. In [BHC], Borel and Harish-Chandra proved that

Theorem 2.2.1 (Borel and Harish-Chandra, original form)**.** *Arithmetic subgroups of algebraic matrix groups defined over $\mathbb{Q}$ are finitely generated.*

Later on, Grunewald and Segal proposed in [GS] to say that an algebraic matrix group G is explicitely given if it is explicitely given a finite set of polynomials with rational coefficients defining it, and, if this is the case, to say that an arithmetic subgroup Γ of G is explicitely given if

- it is contained in $G_{\mathbb{Z}}$,
- an upper bound for the index of Γ in $G_{\mathbb{Z}}$ is given, and

- an effective procedure is given to decide, for each $g \in G_{\mathbb{Z}}$, whether of not $g \in \Gamma$.

It should be noticed that the first requirement is not too severe. In fact,

Proposition 2.2.1. *Let G be an algebraic matrix subgroup of some* $\mathrm{GL}_m(\mathbb{C})$ *defined over $\mathbb{Q}$, and let Γ be an arithmetic subgroup of G. Then there exists $X \in$* $\mathrm{GL}_m(\mathbb{Q})$ *such that G^X is an algebraic matrix subgroup of* $\mathrm{GL}_m(\mathbb{C})$ *and that Γ^X is an arithmetic subgroup of G^X which is contained in $(G^X)_{\mathbb{Z}}$.*

In the same article, improving the techniques used in [BHC] to prove Theorem 2.2.1, they described an algorithm that, beginning with an explicitely given algebraic matrix group G and an explicitely given arithmetic subgroup Γ of G, computes a finite set of generators for Γ. As the same authors pointed out in section “Effectiveness” of [GS], their declared aim was to show that such a computation is, at least in principle, feasible, and no attempt was made to make it as efficient as possible. And unfortunately it appears to be extremely hard to use their algorithm in practice. Further, again Grunewald and Segal showed in [GS2] that, apart from its intrinsic interest, an algorithm for computing a finite set of generators of an explicitely given arithmetic subgroup of an explicitely given algebraic matrix group defined over $\mathbb{Q}$ could be employed as a part of an algorithm for testing isomorphism of finitely generated nilpotent groups.

As we did in the case of algebraic matrix groups defined over $\mathbb{Q}$, it is possible to introduce the notion of arithmetic subgroup of an affine algebraic group $\mathbf{G}$ over $\mathbb{Q}$. In fact, suppose that V is a finite dimensional vector space over $\mathbb{Q}$ on which $\mathbf{G}$ acts faithfully, and that L is a full dimensional lattice of V. Then the group $\mathbf{G}(\mathbb{Q})$ of the rational points of $\mathbf{G}$ acts on V, and it makes sense to consider the normalizer of L with respect to this action. Let us denote it by $\mathbf{G}_L$. Then any subgroup Γ of $\mathbf{G}(\mathbb{Q})$ such that $\Gamma \cap \mathbf{G}_L$ has finite index in both Γ and $\mathbf{G}_L$ will be called an arithmetic subgroup. This notion is both interesting and well-defined since, on one hand, it is well known that any affine algebraic group admits a faithful finite dimensional representation, and, on the other hand, we have that the set of arithmetic subgroups does not depend on the choice of the linear representation, as long as it is faithful, and of the lattice, as long as it is full dimensional. For a proof of the latter statement, see [Mi2], expecially Proposition 28.8. Also, algebraic matrix groups, affine algebraic groups and their arithmetic subgroups are strictly related. In fact, by results in Section 2.1 we have that if $\mathbf{G}$ is an algebraic subgroup of some GL_m over $\mathbb{Q}$, then $\mathbf{G}(\mathbb{C})$ is an algebraic matrix subgroup of $\mathrm{GL}_m(\mathbb{C})$ defined over $\mathbb{Q}$, and that in this way we obtain a bijection between algebraic subgroups of GL_m over $\mathbb{Q}$ and algebraic matrix subgroups of $\mathrm{GL}_m(\mathbb{C})$ defined over $\mathbb{Q}$. Even more, it is easy to check that, if we put

$$G = \mathbf{G}(\mathbb{C}),$$

then the group of the rational points of $\mathbf{G}$ is $G_{\mathbb{Q}}$, and, with respect to the natural action of $\mathbf{G}$ on $\mathbb{Q}^m$, we have that

$$\mathbf{G}_{\mathbb{Z}^m} = G_{\mathbb{Z}}.$$

This shows that the sets of arithmetic subgroups of $\mathbf{G}$ and of G coincide. Also, it is well known that any affine algebraic group over $\mathbb{Q}$ is isomorphic to an algebraic subgroup of some GL_m over $\mathbb{Q}$. Altogether, we conclude that Theorem 2.2.1 is equivalent to

Theorem 2.2.2 (Borel and Harish-Chandra, alternative form)**.** *Arithmetic subgroups of affine algebraic groups over $\mathbb{Q}$ are finitely generated.*

2.3 Explicitely given algebraic actions

Let $\mathbf{G}$ be an affine algebraic group over $\mathbb{Q}$ acting faithfully on a finite dimensional $\mathbb{Q}$-vector space V. The action corresponds to a monomorphism of algebraic groups from $\mathbf{G}$ into GL_V. Composing it with the isomorphism between GL_V and $(\bullet \otimes \mathrm{End}(V))^\times$, and then with the inclusion of $(\bullet \otimes \mathrm{End}(V))^\times$ into $\bullet \otimes \mathrm{End}(V)$, we obtain a natural transformation from $\mathbf{G}$ to $\bullet \otimes \mathrm{End}(V)$. Also, let us denote by S the symmetric algebra on the dual of $\mathrm{End}(V)$. We say that a finitely generated commutative $\mathbb{Q}$-algebra A together with a natural isomorphism η from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$ and a morphism of algebras φ from S to A are shadow data for $\mathbf{G}$ and its action on V if

$$\begin{tikzcd}
\mathrm{Hom}(A,\bullet) \arrow[r, "\sharp\circ\varphi"] \arrow[d, "\eta"] & \mathrm{Hom}(S,\bullet) \arrow[d] \\
\mathbf{G} \arrow[r] & \bullet \otimes \mathrm{End}(V)
\end{tikzcd}$$

is commutative, where the right column is the canonical natural isomorphism and the bottom row is the previously constructed natural transformation. Shadow data exist and are essentially unique. In fact, the $\mathbb{Q}$-algebra A and the natural transformation η always exist by definition of affine algebraic group over $\mathbb{Q}$ and, once they have been fixed, by Yoneda lemma there exists a unique morphism of algebras π such that A, η and π are shadow data for $\mathbf{G}$ and its action on V. Also, if a $\mathbb{Q}$-algebra A', a natural isomorphism η' and a morphism of algebras π' form another shadow data for $\mathbf{G}$ and its action on V, then again by Yoneda lemma there exists a unique isomorphism φ of $\mathbb{Q}$-algebras from A to A' such that

$$\begin{tikzcd}
\mathrm{Hom}(A',\bullet) \arrow[rr, "\sharp\circ\varphi"] \arrow[dr, "\eta'"'] & & \mathrm{Hom}(A,\bullet) \arrow[dl, "\eta"] \\
& \mathbf{G} &
\end{tikzcd}$$

and

$$\begin{tikzcd}
& S \arrow[dl, "\pi"'] \arrow[dr, "\pi'"] & \\
A \arrow[rr, "\varphi"] & & A'
\end{tikzcd}$$

are commutative.

Now suppose that the algebra A, the natural transformation η and the morphism of algebras π are shadow data for $\mathbf{G}$ and its action on V. Note that, given a morphism f from S to another $\mathbb{Q}$-algebra R together with the element x of $R \otimes \mathrm{End}(V)$ corresponding to f through the canonical natural isomorphism between $\bullet \otimes \mathrm{End}(V)$ and $\mathrm{Hom}(S, \bullet)$, then x is contained in the image of $\mathbf{G}(R)$ through the natural transformation from $\mathbf{G}$ to $\bullet \otimes \mathrm{End}(V)$ if and only if there exists a morphism f' from A to R such that

$$\begin{tikzcd} S \arrow[r, "\varphi"] \arrow[dr, "f"'] & A \arrow[d, "f'"] \\ & R \end{tikzcd}$$

is commutative and, if this is the case, then f' is unique and η sends it to the unique element of $\mathbf{G}(R)$ whose image in $R \otimes \operatorname{End}(V)$ is x. We say that the shadow data A, η and φ are given explicitely if they are known to the extent that enables us to compute

- a finite set of generators for the kernel of φ,
- for any algebra R and any $x \in \operatorname{Hom}(A, R)$, the element of $\mathbf{G}(R)$ corresponding to x through η, and,
- for any algebra R and any morphism f from S to R such that there exists a morphism f' from A to R such that $f = f' \circ \varphi$, the morphism f' itself.

As a prototypical example, suppose that $\mathbf{G}$ is an algebraic subgroup of some GL_m with its natural action on $\mathbb{Q}^m$. Also, let $\mathbb{Q}[\hat{X}]$, det and $\mathbb{Q}[\hat{X}]_{\det}$ be as in Section 2.1, let $\mathfrak{j}$ be an ideal of $\mathbb{Q}[\hat{X}]_{\det}$ and η a natural isomorphism from $\operatorname{Hom}(A, \bullet)$ to $\mathbf{G}$ such that

$$\begin{tikzcd} \operatorname{Hom}(A, \bullet) \arrow[r, "\sharp\circ\pi"] \arrow[d, "\eta"] & \operatorname{Hom}(\mathbb{Q}[\hat{X}]_{\det}, \bullet) \arrow[d] \\ \mathbf{G} \arrow[r] & \mathrm{GL}_m \end{tikzcd}$$

is commutative, where $A = \mathbb{Q}[\hat{X}]_{\det}/\mathfrak{j}$, π is the projection of $\mathbb{Q}[\hat{X}]_{\det}$ onto A, the bottom row is the inclusion, and the right column is the canonical natural isomorphism. By Yoneda lemma, $\mathfrak{j}$ and η exist and are unique. Also, let S now denote the symmetric algebra on the dual of $\operatorname{End}(\mathbb{Q}^m)$, and let us denote by φ the map given by composition of

$$S \to \mathbb{Q}[\hat{X}] \to \mathbb{Q}[\hat{X}]_{\det} \xrightarrow{\pi} A,$$

where the arrow on the left is the isomorphism with respect to the canonical basis of $\mathbb{Q}^m$ and the central arrow is the localization map. Then it is easy to check that A, η and φ are shadow data for $\mathbf{G}$ and its action on $\mathbb{Q}^m$. In addition, if we have at hand a finite set of generators $f_1, \ldots, f_n$ for the contraction of $\mathfrak{j}$ throught the localization map from $\mathbb{Q}[\hat{X}]$ to $\mathbb{Q}[\hat{X}]_{\det}$, then the shadow data are explicitely given. Indeed, the images of $f_1, \ldots, f_n$ through the isomorphism between S and $\mathbb{Q}[\hat{X}]$ with respect to the canonical basis of $\mathbb{Q}^m$ form a finite set of generators for the kernel of φ. Also, for any algebra R and any $x \in \operatorname{Hom}(A, R)$, the image of x through η is the image throught the canonical isomorphism between $\operatorname{Hom}(\mathbb{Q}[\hat{X}])_{\det}, \bullet)$ and GL_m of the map given by composition of

$$\mathbb{Q}[\hat{X}]_{\det} \to A \xrightarrow{x} R,$$

where the left arrow is the canonical projection. Further, let us denote by $e_1, \ldots, e_m$ the canonical basis of $\mathbb{Q}^m$, and for every i and j between 1 and m, by e_{ij} the unique endomorphism of $\mathbb{Q}^m$ sending e_i to e_j and all the other elements of the canonical basis of $\mathbb{Q}^m$ to 0. Of course, the set of the e_{ij} for i and j between 1 and m is a basis for $\mathrm{End}(\mathbb{Q}^m)$. Let us denote by e_{ij}^* the elements of the basis for $\mathrm{End}(\mathbb{Q}^m)^*$ which is dual to it. Then it is easy to check that for every algebra R and every morphism f from S to R such that there exists a morphism f' from A to R with $f = f' \circ \varphi$, f' is the unique morphism sending $X_{ij} + \mathfrak{j}$ to $f(e_{ij})$ for any i and j between 1 and m, and the inverse of $\det + \mathfrak{j}$ to the inverse of

$$\sum_{\sigma \in S_m} \mathrm{sgn}(\sigma) f(e_{1\sigma(1)}) \cdots f(e_{m\sigma(m)}),$$

where S_m is the symmetric group of $\{1, \ldots, m\}$ and sgn is the sign morphism.

Finally, suppose that A, η and φ are explicitely given. If we are given an element x in $R \otimes \mathrm{End}(V)$ which is known to be contained in the image of $\mathbf{G}(R)$ through the natural transformation from $\mathbf{G}$ to $\bullet \otimes \mathrm{End}(V)$, then it is possible to compute the element of $\mathbf{G}(R)$ whose image in $R \otimes \mathrm{End}(V)$ is x. In fact, we already noticed that the morphism f from S to R corresponding to x through the canonical isomorphism between $\mathrm{Hom}(S, \bullet)$ and $\bullet \otimes \mathrm{End}(V)$ factors through φ. In our hypothesis, we can compute the morphism f' from A to R such that $f = f' \circ \varphi$ and, in turn, the element of $\mathbf{G}(R)$ corresponding to it through η, which is of course the element we were searching for.

2.4 The problem we are concerned about

The problem of computing a finite set of generators for an explicitely given arithmetic subgroup of an explicitely given algebraic matrix group defined over $\mathbb{Q}$ admits as a special case the problem of computing a finite set of generators for $G_{\mathbb{Z}}$ starting from an algebraic matrix group G defined over $\mathbb{Q}$. Therefore the algorithm by Grunewald and Segal described in Section 2.2 is in particular a solution to the latter problem. Unfortunately, it turns out that it is not practical even in this particular case. Also, it should be noticed that the former problem is actually only slightly more difficult than the latter. In fact, let Γ be an explicitely given arithmetic subgroup of an algebraic matrix group G defined over $\mathbb{Q}$, let $g_1, \ldots, g_n$ be a finite set of generators for $G_{\mathbb{Z}}$, d an upper bound for the index of Γ in $G_{\mathbb{Z}}$, and put

$$W = \{w(g_1, \ldots, g_n) \mid w \text{ is a word in } n \text{ symbols of length at most } d\}.$$

It is well-known that W contains a transversal for Γ in $G_{\mathbb{Z}}$. Also, let us choose an order on W and for every element, starting from the smallest and proceding toward the biggest, let us check if it is in the same coset of $G_{\mathbb{Z}}$ with respect to Γ of a smaller element of W and, if this is the case, let us through it away. Clearly enough, the remaining elements form a transversal T for Γ in $G_{\mathbb{Z}}$. Of course, in order to check if two elements w and w' of W are in the same coset, it is enough to check if $w^{-1}w'$ is in Γ. Therefore, being Γ explicitely given, we can compute T effectively. Further, let us consider the set X of elements of the form

$$tg_i\tau^{-1},$$

where $t \in T$, i is between 1 and n, and τ is the unique element of T lying in the same coset in which tg_i lies. With techniques similar to those used to compute T, it is possible to compute X effectively. Further, by Schreier lemma, X is a finite set of generators for Γ. Therefore a practical algorithm solving the latter problem is likely to lead to a practical algorithm solving the former problem.

In view of Theorem 2.2.2, it makes sense to ask whether there exists an algorithm that, beginning with an affine algebraic group $\mathbf{G}$ over $\mathbb{Q}$ together with a faithful action on a finite dimensional $\mathbb{Q}$-vector space V, a full-dimensional lattice L of V and with explicitely given shadow data for $\mathbf{G}$ and its action on V, computes a finite set of generators for the normalizer $\mathbf{G}_L$ of L with respect to the action of $\mathbf{G}(\mathbb{Q})$ on V. It turns out that the answer is affirmative. In fact, such a problem is equivalent to that of computing a finite set of generators for $G_{\mathbb{Z}}$ starting from an explicitely given algebraic matrix group G defined over $\mathbb{Q}$. Indeed, suppose we have a solution for the latter problem. Also, let $\mathbf{G}$, V and L be as before, and suppose that the algebra A, the natural transformation η and the morphism of algebras φ are explicitely given shadow data for $\mathbf{G}$ and its action on V. Let us denote by m the dimension of V. Also, let $x_1, \ldots, x_m$ be both a basis of V and of L. The faithful action of $\mathbf{G}$ on V corresponds to a monomorphism of algebraic groups from $\mathbf{G}$ into GL_V. Composing it with the isomorphism between GL_V and GL_m with respect to $x_1, \ldots, x_m$, we obtain a monomorphism of algebraic groups from $\mathbf{G}$ to GL_m. Let us denote by $\mathbf{G}'$ its image, and by ξ the unique isomorphism of algebraic groups from $\mathbf{G}$ to $\mathbf{G}'$ such that

$$\begin{tikzcd} \mathbf{G} \arrow[r] \arrow[d, "\xi"'] & \mathrm{GL}_m \\ \mathbf{G}' \arrow[ur] & \end{tikzcd}$$

is commutative, where the horizontal arrow is the previously constructed monomorphism of algebraic groups, and the diagonal arrow is the inclusion. Also, let $\mathbb{Q}[\hat{X}]$, det and $\mathbb{Q}[\hat{X}]_{\det}$ be as in Section 2.1. By Yoneda lemma, there exists a unique morphism of algebras π from $\mathbb{Q}[\hat{X}]_{\det}$ to A such that

$$\begin{tikzcd} \mathrm{Hom}(A, \bullet) \arrow[r, "\sharp\circ\pi"] \arrow[d, "\xi\circ\eta"] & \mathrm{Hom}(\mathbb{Q}[\hat{X}]_{\det}) \arrow[d] \\ \mathrm{G}' \arrow[r] & \mathrm{GL}_m \end{tikzcd}$$

is commutative, where the bottow row is the inclusion and the right column is the canonical natural isomorphism. Also, let us denote by S the symmetric algebra on the dual of $\mathrm{End}(V)$, and by i the algebras isomorphism from $\mathbb{Q}[\hat{X}]$ to S with respect to $x_1, \ldots, x_m$. Then it is easy to see that

$$\begin{tikzcd} \mathbb{Q}[\hat{X}] \arrow[r] \arrow[d, "i"] & \mathbb{Q}[\hat{X}]_{\det} \arrow[d, "\pi"] \\ S \arrow[r, "\varphi"] & A \end{tikzcd}$$

is commutative, where the top row is the localization map. Let us put

$$G = \mathbf{G}'(\mathbb{C}).$$

Then by results on Section 2.1, we have that G is an algebraic matrix subgroup of $\mathrm{GL}_m(\mathbb{C})$ defined over $\mathbb{Q}$ by the images through the inverse of i of any finite set of generators for the kernel of φ. Therefore in our hypothesis G is given explicitely, hence we are able to compute a finite set of generators $g_1, \ldots, g_n$ for $G_{\mathbb{Z}}$. Of course, any of the g_i is an element of $\mathrm{M}_m(\mathbb{Q})$. Also, it is easy to check that the endomorphism of V whose matrix with respect to $x_1, \ldots, x_m$ is g_i, is contained in the image of $\mathbf{G}(\mathbb{Q})$ through the natural transformation from $\mathbf{G}$ to $\bullet \otimes \mathrm{End}(V)$ described in Section 2.3. Therefore by our assumptions we are able to compute its preimage h_i. Finally, it follows easily that the image of any h_i through ξ is g_i, and therefore that $h_1, \ldots, h_n$ is a finite set of generators for $\mathbf{G}_L$. Conversely, suppose we have at hand an algorithm solving the former problem, and that $f_1, \ldots, f_n$ are explicitely given polynomials in $\mathbb{Q}[\hat{X}]$ defining an algebraic matrix subgroup G of $\mathrm{GL}_m(\mathbb{C})$. By results of Section 2.1, there exists a unique algebraic subgroup $\mathbf{G}$ of GL_m such that $\mathbf{G}(\mathbb{C}) = G$. The canonical action of $\mathbf{G}$ on $\mathbb{Q}^m$ associates to $\mathbb{Q}$ an action of $\mathbf{G}(\mathbb{Q})$ on $\mathbb{Q}^m$. As already noticed in Section 2.2, the normalizer of $\mathbb{Z}^m$ with respect to it is $G_{\mathbb{Z}}$. Therefore it is enough to provide explicitely given shadow data for $\mathbf{G}$ together with its action on $\mathbb{Q}^m$. Then, applying the algorithm we have at hand, we will obtain a finite set of generators for $G_{\mathbb{Z}}$. To this end, let us denote by $\mathfrak{i}$ the radical of the ideal of $\mathbb{Q}[\hat{X}]$ generated by $f_1, \ldots, f_n$, by $\mathfrak{j}$ the extension of $\mathfrak{i}$ through the localization map from $\mathbb{Q}[\hat{X}]$ to $\mathbb{Q}[\hat{X}]_{\det}$, and let us put $A = \mathbb{Q}[\hat{X}]_{\det}/\mathfrak{j}$. Since the contraction of $\mathfrak{j}$ through the localization map from $\mathbb{Q}[\hat{X}]$ to $\mathbb{Q}[\hat{X}]_{\det}$ is again $\mathfrak{i}$, by results of Section 2.1 we have that there exists a unique natural transformation η from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$ such that

$$\begin{tikzcd} \mathrm{Hom}(A, \bullet) \arrow[r, "\sharp \circ \pi"] \arrow[d, "\eta"] & \mathrm{Hom}(\mathbb{Q}[\hat{X}]_{\det}, \bullet) \arrow[d] \\ \mathbf{G} \arrow[r] & \mathrm{GL}_m \end{tikzcd}$$

is commutative, where π is the projection of $\mathbb{Q}[\hat{X}]_{\det}$ onto A, the bottom row is the inclusion, and the right column is the canonical natural isomorphism. Also, η is a natural isomorphism. Let S now denote the symmetric algebra on the dual of $\mathrm{End}(\mathbb{Q}^m)$. By results of Section 2.3 we have that A and η together with the map φ given by composition of

$$S \to \mathbb{Q}[\hat{X}] \to \mathbb{Q}[\hat{X}]_{\det} \to A,$$

where the left arrow is the isomorphism with respect to the canonical basis of $\mathbb{Q}^m$, the central arrow is the localization map and the right arrow is the canonical projection, are shadow data for $\mathbf{G}$ and its action on $\mathbb{Q}^m$. Also, there exist well-known algorithms for computing a finite set of generators for $\mathfrak{i}$ starting from $f_1, \ldots, f_n$. For references, see [BW]. Therefore, again by results of Section 2.3, the shadow data are given explicitely.

Altogether, results of this section and of Section 2.2 should convince that providing a practical algorithm that, beginning with an affine algebraic group $\mathbf{G}$ over $\mathbb{Q}$ together with a faithful action on a finite dimensional $\mathbb{Q}$-vector space V, a full-dimensional lattice L of V and with explicitely given shadow data for $\mathbf{G}$ and its action on V, computes a finite set of generators for the normalizer $\mathbf{G}_L$ of L with respect to the action of $\mathbf{G}(\mathbb{Q})$ on V, is an interesting problem. In the next two chapters, we will solve it in two special cases.

Chapter 3

The unipotent case

In this chapter we provide an algorithm solving the problem described in Chapter 2 in the special case in which the given algebraic group is unipotent. The first five sections are devoted to prove some auxiliary results, which are used in Section 3.6 to provide, on one hand, an independent proof of the theorem 2.2.2 in the special case of the unipotent groups, and, on the other hand, to describe the algorithm and to prove its correctness. The last section gives some evidences about the practicality of the algorithm.

3.1 Lattices and complements

Let V be a finite dimensional vector space over $\mathbb{Q}$ and L a full-dimensional lattice of V.

Lemma 3.1.1. *The function from the set of pure subgroups of L to the set of subspaces of V sending any pure subgroup M to the subspace $\langle M\rangle_{\mathbb{Q}}$ of V generated by M is bijective, and its inverse sends any subspace W on V to $W \cap L$. Given subgroups M and M',*

$$\langle M \cap M'\rangle_{\mathbb{Q}} = \langle M\rangle_{\mathbb{Q}} \cap \langle M'\rangle_{\mathbb{Q}} \quad \textit{and} \quad \langle M + M'\rangle_{\mathbb{Q}} = \langle M\rangle_{\mathbb{Q}} + \langle M'\rangle_{\mathbb{Q}}.$$

Proof. It is immediate to show that for any subspace W of V, $W \cap L$ is a pure subgroup of L. Therefore the two functions are well-defined. Now suppose that M is any subgroup of V. Then an easy argument shows that $\langle M\rangle_{\mathbb{Q}}/M$ is precisely the torsion subgroup of V/M. This fact has many useful consequences. As a first thing, let us suppose that M is a subgroup of L. Then $\langle M\rangle_{\mathbb{Q}} \cap L/M$ is the intersection of the torsion subgroup of V/M with L/M, that is to say, it is the torsion subgroup of L/M. In particular, if M is a pure subgroup of L, then it is equal to $\langle M\rangle_{\mathbb{Q}} \cap L$. Secondly, let us consider a subspace W of V. Then

$$\langle W \cap M\rangle_{\mathbb{Q}} = W \cap \langle M\rangle_{\mathbb{Q}}.$$

It is easy to see that the former subspace is included in the latter. To prove the reverse inclusion, it is enough to show that

$$\frac{W \cap \langle M\rangle_{\mathbb{Q}}}{W \cap M}$$

is a torsion group. This is easy recalling that $\langle M\rangle_{\mathbb{Q}}/M$ is. In particular, $\langle W\cap L\rangle_{\mathbb{Q}}$ is equal to W. Together, these two facts show that the functions we built are one the inverse of the other. A proof of the remaining two equalities can be given with similar arguments. $\square$

Now suppose that U and W are subspace of V, and that $U \leq W$. Then there exist a complement U' of U and a complement W' of W in V such that

$$W' \leq U' \ , \quad (U\cap L)+(U'\cap L)=L \quad \text{and} \quad (W\cap L)+(W'\cap L)=L.$$

In fact, by Lemma 3.1.1 we have that $W\cap L$ is a pure subgroup of L, hence it admits a complement M in L. Similarly we have that $L\cap U$ is a pure subgroup of L, thus it is also a pure subgroup of $W\cap L$, and therefore it admits a complement in $W\cap L$. Let us denote by M' the internal sum of M with such a complement. Of course, $M \leq M'$ and $M'+(U\cap L)=L$. Also, it is easy to see that $M'\cap(M+(U\cap L))=M$. In turn, applying Dedekind modular law, we have that $M'\cap(U\cap L)\leq M$. Since $M'\cap(U\cap L)$ is also contained in $W\cap L$, it is the zero submodules. Therefore M' is a complement of $U\cap L$ in L. Exploiting again Lemma 3.1.1 it is easy to see that we can choose $\langle M'\rangle_{\mathbb{Q}}$ as U' and $\langle M\rangle_{\mathbb{Q}}$ as W'.

3.2 A lemma on T-groups

Let n be a strictly positive integer. For any non-zero $x=(x_1,\dots,x_n)$ in $\mathbb{Z}^n$, let us define its height as the minimum j between 1 and n such that $x_j\neq 0$, and its leading coefficient as x_j, where j is its height. Also, let A be an abelian group, and let $a_1,\dots,a_n\in A$. Then there exists a unique morphism of groups from $\mathbb{Z}^n$ sending the i-th element of the canonical basis of $\mathbb{Z}^n$ to a_i for any i between 1 and n. We will refer to its kernel L as the relation lattice for $a_1,\dots,a_n$. Further, given a basis $x^{(1)},\dots,x^{(m)}$ of L, we say that it is in Hermite normal form if

$$\begin{pmatrix} x_1^{(1)} & \cdots & x_n^{(1)} \\ \vdots & & \vdots \\ x_1^{(m)} & \cdots & x_n^{(m)} \end{pmatrix} \in M_{m\times n}(\mathbb{Z})$$

is, where

$$x^{(i)}=(x_1^{(i)},\dots,x_n^{(i)}).$$

This means that there exist

$$1\leq i_1<\cdots<i_m\leq n$$

such that

$$x_i^{(j)}=0$$

for all $j=1,\dots,m$ and all $1\leq i<i_j$, and that

$$0\leq x_{i_j}^{(k)}<x_{i_j}^{(j)}$$

for every $1\leq k<j\leq m$. If this is the case, the $i_1,\dots,i_m$ are unique, and they are the only possible heights of the non-zero elements in L. We will refer to

them as the heigths of $x^{(1)}, \dots, x^{(m)}$. Also, if a non-zero x in L has height i_j, then its leading coefficient is a non-zero multiple of $x^{(j)}_{i_j}$. Finally, note that it is well-known that L admits a unique basis in Hermite normal form, and that there exists well-known algorithm to compute it beginning from any finite set of generators for L. For more details, see for example [Si].

Lemma 3.2.1. *Let G be a T-group, A an abelian group, and let φ be a group morphism from G to A. Further, let $g_1, \dots, g_n$ be a T-sequence for G, and let $x^{(1)}, \dots, x^{(m)}$ be the basis in Hermite normal form for the relation lattice of $\varphi(g_1), \dots, \varphi(g_n)$. For any j between 1 and m, set*

$$k_j = g_1^{x_1^{(j)}} \cdots g_n^{x_n^{(j)}}.$$

Then $k_1, \dots, k_m$ is a T-sequence for the kernel of φ.

Proof. Let us set

$$G_i = \langle g_i, \dots, g_n \rangle \text{ for } i \text{ between 1 and } n, \quad \text{and} \quad G_{n+1} = 1.$$

Also, set

$$K_i = \langle k_i, \dots, k_m \rangle \text{ for } i \text{ between 1 and } m, \quad \text{and} \quad K_{m+1} = 1.$$

Now let us denote by $i_1, \dots, i_m$ the heights of $x^{(1)}, \dots, x^{(m)}$. Also, it is convenient to set

$$i_0 = 0 \quad \text{and} \quad i_{m+1} = n + 1.$$

Then it is enough to prove that for every j between 1 and $m + 1$, and every l between $i_{j-1} + 1$ and i_j,

$$\ker\varphi \cap G_l = K_j.$$

Indeed, suppose that the previous equalities hold. Recall that

$$G = G_1 \geq \cdots \geq G_i \geq \cdots \geq G_{m+1} = 1$$

is a central series for G with infinite cyclic factors. Then

$$K_1 = \ker\varphi \cap G_{i_0+1} = \ker\varphi \cap G_1 = \ker\varphi \cap G = \ker\varphi.$$

Also, for every j between 1 and $m + 1$, G_{i_j} is normal in G, hence

$$K_j = \ker\varphi \cap G_{i_j} \trianglelefteq \ker\varphi \cap G = \ker\varphi.$$

This shows that

$$K = K_1 \geq \cdots \geq K_i \geq \cdots \geq K_{m+1} = 1$$

is a normal series for $\ker\varphi$. Further, for every j between 1 and m, the map given by composition of

$$\ker\varphi \to G \to \frac{G}{G_{i_j+1}}$$

where the left arrow is the inclusion and the right arrow is the projection, has kernel

$$\ker\varphi \cap G_{i_j+1} = K_{j+1}.$$

Hence it factors through a group monomorphism from $\ker\varphi/K_{j+1}$ to G/G_{i_j+1}. The image of K_j/K_{j+1} through it is

$$\frac{K_j G_{i_j+1}}{G_{i_j+1}} = \frac{(\ker\varphi \cap G_{i_j})G_{i_j+1}}{G_{i_j+1}} = \frac{(\ker\varphi\ G_{i_j+1}) \cap G_{i_j}}{G_{i_j+1}} \leq \frac{G_{i_j}}{G_{i_j+1}},$$

and the image of $k_j K_{j+1}$ is $g_{i_j}^{x^{(j)}_{i_j}} G_{i_j+1} \neq 1$. This shows that the series is central and with infinite cyclic factors.

So we have to prove the previous equalities. It is clear that for every j between 1 and $m+1$, and every $i_{j-1}+1 \leq l < l' \leq i_j$,

$$\ker\varphi \cap G_l \supseteq \ker\varphi \cap G_{l'} \supseteq K_j,$$

and it remains to prove the reverse inclusions. We proceed by induction on j. Let us consider the base case $j = m+1$. Then K_j is trivial, and all we have to show is that for every l between i_m+1 and $n+1$, $\ker\varphi \cap G_l$ is trivial, too. Again, we proceed by induction on l. In the base case $l = n+1$, it is obviously true. Now let l be between i_m+1 and n and suppose that $\ker\varphi \cap G_{l+1}$ is trivial. Let $g \in \ker\varphi \cap G_l$. Then $g = g_l^e h$ for some $e \in \mathbb{Z}$ and $h \in G_{l+1}$, and

$$\varphi(g_l)^e + \varphi(h) = 0$$

Since $h \in \langle g_{l+1}, \ldots, g_n \rangle$, then $\varphi(h) \in \langle \varphi(g_{l+1}), \ldots, \varphi(g_n) \rangle$. Thus if $e \neq 0$, then there would exist an element in the relation lattice with height l, which is impossible since l is not among the heights of $x^{(1)}, \ldots, x^{(m)}$. Hence $e = 0$, and g is equal to h, which is in $\ker\varphi \cap G_{l+1}$. Therefore $g = 1$ by the inductive hypothesis. This concludes the case $j = m+1$. Now let j be between 1 and m, and suppose that for every l between i_j+1 and i_{j+1},

$$\ker\varphi \cap G_l = K_j.$$

In this case we have to show that for every l between $i_{j-1}+1$ and i_j,

$$\ker\varphi \cap G_l = K_j,$$

and again we proceed by induction on l. Let us just consider the base case $l = i_j$, the inductive step being similar to the one in the case $j = m+1$. Let $g \in \ker\varphi \cap G_{i_j}$. Then $g = g_{i_j}^e h$ for some $e \in \mathbb{Z}$ and some $h \in G_{i_j+1}$. If $e = 0$ then $g \in G_{i_j+1}$ and we conclude by inductive hypothesis that $g \in K_{j+1}$. Now let us suppose that $e \neq 0$. Arguing as before, the relation lattice contains an element of height i_j and leading coefficient e. Thus $x^{(j)}_{i_j}$ divides e. Let us denote by f the quotient. Then $gG_{i_j+1} = k_i^f G_{i_j+1}$, hence by inductive hypothesis $gk_j^{-f} \in \ker\varphi \cap G_{i_j+1} = K_{j+1}$, hence finally $g \in K_j$. □

3.3 Algebraic subgroups of vector spaces

Let V be a finite dimensional vector space over $\mathbb{Q}$, and let us denote it by $\bullet \otimes V$ the affine space on V. Also, let $\mathbf{G}$ be an algebraic subgroup of $\bullet \otimes V$. Then

Lemma 3.3.1. *We have that* $\mathbf{G}$ *is equal to* $\bullet \otimes U$ *for some subspace* U *of* V.

Proof. For any ideal $\mathfrak{a}$ of $\mathrm{S}(V^*)$ let us denote by $\mathrm{V}_{\mathfrak{a}}$ the algebraic subset of $\mathrm{Hom}(\mathrm{S}(V^*), \bullet)$ that to any algebra R associates

$$\mathrm{V}_{\mathfrak{a}}(R) = \{\varphi \in \mathrm{Hom}(\mathrm{S}(V^*), R) \mid \mathfrak{a} \leq \ker\varphi\}.$$

It is easy to check that in this way we obtain a bijection between ideals of $\mathrm{S}(V^*)$ and algebraic subsets of $\mathrm{Hom}(\mathrm{S}(V^*), \bullet)$. Also, $V_{\mathfrak{a}}$ is an algebraic subgroup of $\mathrm{Hom}(\mathrm{S}(V^*), \bullet)$ if and only if $\mathfrak{a}$ is an Hopf ideal of $\mathrm{S}(V^*)$ with respect to its canonical structure of Hopf algebra, that is to say, if

$$\Delta(\mathfrak{a}) \subseteq \mathrm{S}(V^*) \otimes \mathfrak{a} + \mathfrak{a} \otimes \mathrm{S}(V^*) \ ,$$

where Δ is the co-multiplication of $\mathrm{S}(V^*)$. Also, if $\mathfrak{a}$ is an ideal of $\mathrm{S}(V^*)$ generated by $\mathfrak{a} \cap V^*$, then the image of $V_{\mathfrak{a}}$ through the isomorphism between $\mathrm{Hom}(\mathrm{S}(V^*), \bullet)$ and $\bullet \otimes V$ is precisely $\bullet \otimes U$, where U is the orthogonal of $\mathfrak{a} \cap V^*$ with respect to the standard bilinear form between V and its dual. Therefore it is enough to show that any Hopf ideal $\mathfrak{a}$ of $\mathrm{S}(V^*)$ is generated by $\mathfrak{a} \cap V^*$.

To this end, let us denote by $\mathfrak{b}$ the ideal generated by $\mathfrak{a} \cap V^*$. Of course it is contained in $\mathfrak{a}$. Since it is generated by $\mathfrak{b} \cap V^*$, the discussion in the previous paragraph shows that it is an Hopf ideal of $\mathrm{S}(V^*)$. Therefore it is easy to check that there exists a unique structure of Hopf algebra on $\mathrm{S}(V^*)/\mathfrak{b}$ making the canonical projection of $\mathrm{S}(V^*)$ onto $\mathrm{S}(V^*)/\mathfrak{b}$ into a morphism of Hopf algebras. Also, if we let U now denote the orthogonal of $\mathfrak{b} \cap V^*$, then the canonical epimorphism from $\mathrm{S}(V^*)$ to $\mathrm{S}(U^*)$ factor through an isomorphism between $\mathrm{S}(V^*)/\mathfrak{b}$ and $\mathrm{S}(U^*)$. With respect to the standard structure of Hopf algebra on $\mathrm{S}(U^*)$, it is an isomorphism of Hopf algebras. Therefore the image of the Hopf ideal $\mathfrak{a}/\mathfrak{b}$ through it is an Hopf ideal $\mathfrak{c}$ of $\mathrm{S}(U^*)$, and $\mathfrak{c} \cap U^*$ is the zero subspace. It is enough to show that then $\mathfrak{c}$ is the zero ideal.

By contradiction, suppose that $\mathfrak{c}$ is not zero. Then there exists $c \in \mathfrak{c}$ which is of minimum degree among the non-zero elements in $\mathfrak{c}$ with respect to the standard grading on $\mathrm{S}(U^*)$. Since $\mathfrak{c} \cap U^* = 0$, its degree is at least 2. Now let us denote by Δ the co-multiplication on $\mathrm{S}(U^*)$, and by π the projection of $\mathrm{S}(U^*)$ onto $\mathrm{S}(U^*)/\mathfrak{c}$. Since $\mathfrak{c}$ is an Hopf ideal,

$$\pi \otimes \pi(\Delta(a) - a \otimes 1 - 1 \otimes a) = 0$$

for any $a \in \mathfrak{a}$. Now let us denote by $u_1, \ldots, u_m$ a basis of U^*. Then the set of elements of the form

$$z_\alpha = \prod_{i=1}^{m} \frac{1}{\alpha_i!} u_i^{\alpha_i}$$

for some $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$, is a basis of $\mathrm{S}(V^*)$. In fact, a stronger statement holds. For any $\alpha \in \mathbb{N}^m$, let us put

$$|\alpha| = \sum_{i=1}^{m} \alpha_i \ , \quad \text{where} \quad \alpha = (\alpha_1, \ldots, \alpha_m).$$

Then the set of the z_α where $|\alpha| = m$ is a basis for the m-th homogeneous component of $\mathrm{S}(U^*)$. Also, this basis is well-suited for dealing with co-multiplication. In fact, for any $\alpha \in \mathbb{N}^m$,

$$\Delta(z_\alpha) = \sum_{\substack{\beta,\gamma \in \mathbb{N}^m \\ \beta+\gamma=\alpha}} z_\beta \otimes z_\gamma.$$

Now let us denote by δ the degree of c. The previous discussion shows that c is equal to

$$\sum_{\alpha\in\mathbb{N}^m} \lambda_\alpha z_\alpha$$

for some unique $\lambda_\alpha \in \mathbb{Q}$, and $\lambda_\alpha = 0$ as soon as $|\alpha| > \delta$. Then a simple computation shows that

$$\Delta(c) - c\otimes 1 - 1\otimes c = -\lambda_0 + \sum_{\substack{\beta,\gamma\in\mathbb{N}^m\\ 0<|\beta|,|\gamma|<\delta}} \lambda_{\beta+\gamma} z_\beta \otimes z_\gamma .$$

Therefore

$$-\lambda_0 + \sum_{\substack{\gamma\in\mathbb{N}^m\\ 0<|\gamma|<\delta}} \left(\sum_{\substack{\beta\in\mathbb{N}^m\\ 0<|\beta|<\delta}} \lambda_{\beta+\gamma}\pi(z_\beta) \right) \otimes \pi(z_\gamma) = 0.$$

By hypothesis $\mathfrak{c}$ does not contain any non-zero element of degree strictly less than δ. Therefore the $\pi(z_\alpha)$ with $|\alpha| < \delta$ are linearly independent, and it follows that both λ_0 and the

$$\sum_{\substack{\beta\in\mathbb{N}^m\\ 0<|\beta|<\delta}} \lambda_{\beta+\gamma}\pi(z_\beta) \text{ , where } \gamma\in\mathbb{N}^m \text{ and } 0<|\gamma|<\delta,$$

are zero. Again exploiting the linear independence of the $\pi(z_\alpha)$ with $|\alpha| < \delta$, we finally deduce tha the $\lambda_{\beta+\gamma}$ are all zero for $\beta, \gamma \in \mathbb{N}^m$ and $0 < |\beta|, |\gamma| < \delta$. Altogether, we conclude that the λ_α are different to zero only if $|\alpha| = 1$. Therefore c lies in $\mathfrak{c} \cap U^*$, which is impossible since the former is different to zero while the latter is the zero subspace. □

3.4 A new representation

Let $\mathbf{G}$ be a unipotent affine algebraic group over $\mathbb{Q}$ acting faithfully on a finite dimensional $\mathbb{Q}$-vector space V, and let L be a full dimensional lattice of V. Also, let

$$0 = V_0 \leq V_1 \leq \cdots \leq V_{m-1} \leq V_m = V$$

be a flag of V with respect to the action of $\mathbf{G}$, and suppose that its length m is at least 2. Further, let us denote by $\mathbf{G}_L$ the normalizer of L with respect to the action of $\mathbf{G}(\mathbb{Q})$ on V. Since V_{m-1} is a $\mathbf{G}$-stable subspace of V, $\mathbf{G}$ acts on it. Similarly, V_1 is $\mathbf{G}$-stable, hence $\mathbf{G}$ acts on V/V_1. It follows that $\mathbf{G}$ acts on their direct sum $V^\star$, too. Let us denote by $\mathbf{N}$ the kernel of the action of $\mathbf{G}$ on $V^\star$. Of course $\mathbf{N}$ acts on V, hence it makes sense to consider the normalizer $\mathbf{N}_L$ of L with respect to the action of $\mathbf{N}(\mathbb{Q})$ on V. Then

Proposition 3.4.1. $\mathbf{N}_L$ *is a central subgroup of* $\mathbf{G}_L$.

Proof. It is enough to prove that $\mathbf{N}(\mathbb{Q})$ is central in $\mathbf{G}(\mathbb{Q})$. Since $\mathbf{G}(\mathbb{Q})$ acts faithfully on V, this amounts to prove that for any $g \in \mathbf{G}(\mathbb{Q})$, any $h \in \mathbf{N}(\mathbb{Q})$ and any $v \in V$, we have $gh.v = hg.v$. Note that h acts as the identity on V/V_1. Therefore $h.v - v \in V_1$. Also, g acts as the identity on V_1, hence

$$g.(h.v - v) = h.v - v.$$

Similarly, since g acts as the identity on V/V_{m-1} and h acts as the identity on V_{m-1},

$$h.(g.v - v) = g.v - v.$$

Now the thesis follows easily. $\square$

Now let us denote by $\mathbf{Q}$ the image of the action of $\mathbf{G}$ on $V^\star$ and by π the epimorphism of algebraic groups from $\mathbf{G}$ to $\mathbf{Q}$. Also, let us put

$$L^\star = (V_{n-1} \cap L) \oplus \frac{V_1 + L}{V_1},$$

and, for every i between 0 and $m-1$,

$$V_i^\star = V_i \oplus \frac{V_{i+1}}{V_1}.$$

Then

Proposition 3.4.2. *The action of* $\mathbf{Q}$ *on* $V^\star$ *is faithful and*

$$0 = V_0^\star \leq \cdots \leq V_i^\star \leq \cdots \leq V_{m-1}^\star = V^\star$$

is a flag for it, of length $m-1$*. Also,* $L^\star$ *is a full dimensional lattice of* $V^\star$*.*

Proof. It is easy to check that the chain consisting of the subspaces $V_i^\star$ of $V^\star$ is a flag for the action of $\mathbf{G}$ on $V^\star$. Since the map that π associates to any $\mathbb{Q}$-algebra R is surjective, the first part of the statement follows. Finally, using results in Section 3.1, it is easy to show that $L^\star$ is a full-dimensional lattice of $V^\star$. The other claims are immediate. $\square$

Further, let us denote by $\mathbf{G}_{L^\star}$ the normalizer of $L^\star$ with respect to the action of the rational points of $\mathbf{G}$ on $V^\star$, and, similarly, by $\mathbf{Q}_{L^\star}$ the normalizer of $L^\star$ with respect to the action of the rational points of $\mathbf{Q}$ on $V^\star$.

According to the results in Section 3.1, there exist a complement V_1' to V_1 in V and a complement V_{m-1}' to V_{m-1} in V such that

$$V_{m-1}' \leq V_1' \ , \quad (V_1 \cap L) + (V_1' \cap L) = L \quad \text{and} \quad (V_{m-1} \cap L) + (V_{m-1}' \cap L) = L.$$

Let us denote by E the vector space of the linear transformations from V_{m-1}' to V_1, and by Λ the subset of E consisting of the linear transformations λ such that $\lambda(V_{m-1}' \cap L) \leq V_1 \cap L$. Then

Proposition 3.4.3. Λ *is a full dimensional lattice of* E*.*

Proof. By results of Section 3.1, $V_{m-1}' \cap L$ is a full dimensional lattice of V_{m-1}', and $V_1 \cap L$ is a full-dimensional lattice of V_1. Therefore $V_{m-1}' \cap L$ has a basis $b_1, \ldots, b_l$ as an abelian group which is also a basis for V_{m-1}' as a vector space. Similarly, $V_1 \cap L$ has a basis $c_1, \ldots, c_k$ as an abelian group which is also a basis for V_1 as a vector space. Now, for any suitable choice of i and j, let $d_{i,j}$ be the unique element of E sending b_i to c_j, and any other element of the considered basis for V_{m-1}' to 0. Then the $d_{i,j}$ form both a basis for Λ as an abelian group, and a basis for E as a vector space. The thesis follows. $\square$

The action of $\mathbf{G}$ on V corresponds to a morphism of algebraic groups from $\mathbf{G}$ to GL_V. In particular, any rational point of $\mathbf{G}$ can be regarded as an automorphism of V. Therefore it makes sense to consider the map ε from $\mathbf{G}(\mathbb{Q})$ to E sending any automorphism of V contained in $\mathbf{G}(\mathbb{Q})$ to the composition of its restriction to V'_{m-1} with the projection of V onto V_1 along the complement V'_1.

Proposition 3.4.4. *Let g be a rational point of $\mathbf{G}$. Then g is in $\mathbf{G}_L$ if and only if it is in $\mathbf{G}_{L^\star}$ and its image through ε is in Λ. In particular, a rational point h of $\mathbf{N}$ is in $\mathbf{N}_L$ if and only if $\varepsilon(h) \in \Lambda$.*

Proof. We will only prove the statement concerning the rational points of $\mathbf{G}$, since the statement about the rational points of $\mathbf{N}$ is just a corollary. Of course, it is enough to prove that for any automorphism φ of V such that V_1 and V_{m-1} are stable under it, we have that L is stable under φ if and only if $V_1 + L$ and $V_{m-1} \cap L$ are, and the image of $V'_{m-1} \cap L$ through the composition of φ with the projection p of V onto V_1 along V'_1 is contained in $V_1 \cap L$. Since L is the direct sum of $V_1 \cap L$ and $V'_1 \cap L$, the image of L through p is contained in $V_1 \cap L$. With this remark at hand, it is easy to see that the three conditions are necessary. Now let us prove that they are also sufficient. In our hypothesis, $\varphi(V'_{m-1} \cap L)$ is contained in the preimage of $V_1 \cap L$ through p, that is to say, in $V'_1 + (V_1 \cap L)$. Also, $\varphi(V'_{m-1} \cap L)$ is contained in $V_1 + L$. Therefore $\varphi(V'_{m-1} \cap L)$ is contained in

$$(V'_1 + (V_1 \cap L)) \cap (V_1 + L),$$

which is equal to L by Dedekind's modular law and recalling that $L \subseteq V'_1 + (V_1 \cap L)$. Since $V_{m-1} \cap L$ is stable under φ, it follows that $\varphi(L) \subseteq L$. Thus it remains to prove the other inclusion. To this end, let $y \in L$. Since $V_1 + L$ is stable under φ, there exist $x \in V_1$ and $y' \in L$ such that

$$\varphi(x) + \varphi(y') = y.$$

We have just shown that $\varphi(y')$ is in L. Therefore also $\varphi(x)$ is. Since V_1 is stable under φ, we even have that $\varphi(x) \in V_1 \cap L$. In particular, $\varphi(x) \in V_{m-1} \cap L$, hence $x \in V_{m-1} \cap L$. Now the thesis follows. $\square$

The group of the rational points of $\mathbf{N}$ acts on the right on the set of the rational points of $\mathbf{G}$ by multiplication. Also,

Proposition 3.4.5. *The restriction of ε to the rational points of $\mathbf{N}$ is a monomorphism of groups with respect to the underlying group structure of the vector space E. In particular,*

$$E \times \mathbf{N}(\mathbb{Q}) \to E \quad , \quad (\lambda, h) \mapsto \lambda + \varepsilon(h)$$

is a right action of $\mathbf{N}(\mathbb{Q})$ on the set E. In this way, ε is a morphism of $\mathbf{N}(\mathbb{Q})$-sets.

Proof. It is enough to show that the restriction of ε to $\mathbf{N}(\mathbb{Q})$ is injective, and that for every $g \in \mathbf{G}(\mathbb{Q})$ and every $h \in \mathbf{N}(\mathbb{Q})$,

$$\varepsilon(gh) = \varepsilon(g) + \varepsilon(h).$$

In turn, in order to prove the first part of this statement it is enough to show that the identity function is the only automorphism of V acting as the identity on both V_{m-1} and on V/V_1, and such that the composition of its restriction to V'_{m-1} with the projection p of V onto V_1 along V'_1 is the zero function. Of course the identity function satisfies all of these properties. Now suppose that φ is another automorphism of V that satisfies them. Also, let $x \in V'_{m-1}$. Since φ acts as the identity on V/V_1, $\varphi(x) - x \in V_1$, hence

$$p(\varphi(x) - x) = \varphi(x) - x.$$

Since $p \circ \varphi$ sends V'_{m-1} to 0 and $x \in \ker p$, it follows that $\varphi(x) = x$, that is to say, φ acts as the identity on V'_{m-1}. Then the first part of the statement follows easily. It remains to prove the second part. To this end, let $x \in V'_{m-1}$. Since h is an automorphism of V acting as the identity on V/V_1, $h(x) - x \in V_1$. Also, g is an automorphism of V acting as the identity on V_1, hence

$$g(h(x) - x) = h(x) - x.$$

Since V_{m-1} is contained in V_1, we have that $p(x) = 0$. Therefore applying p to both sides of the previous identity, we obtain that

$$p \circ g \circ h(x) = p \circ g(x) + p \circ h(x).$$

Now the thesis follows easily. □

Since $\mathbf{G}$ and $\mathbf{Q}$ are unipotent, the rational points of $\mathbf{Q}$ are the orbit space for the action of $\mathbf{N}(\mathbb{Q})$ on $\mathbf{G}(\mathbb{Q})$. Now let us denote by F the image of the rational points of $\mathbf{N}$ through ε. According to the previous proposition, it is a subgroup of E, E/F is the orbit space for the action of $\mathbf{N}(\mathbb{Q})$ on E, and there exists a unique map $\hat{\epsilon}$ from $\mathbf{Q}(\mathbb{Q})$ to E/F such that

$$\begin{tikzcd}
\mathbf{G}(\mathbb{Q}) \arrow[r, "\varepsilon"] \arrow[d, "\pi"] & E \arrow[d] \\
\mathbf{Q}(\mathbb{Q}) \arrow[r, "\hat{\varepsilon}"] & E/F
\end{tikzcd}$$

is commutative, where the right column is the canonical projection. In particular, we have at hand the map Ψ given by composition of

$$\mathbf{Q}_{L^\star} \to \mathbf{Q}(\mathbb{Q}) \xrightarrow{\hat{\varepsilon}} \frac{E}{F} \to \frac{E}{F + \Lambda},$$

where the left arrow is the inclusion and the right arrow is the canonical projection. We have that

Proposition 3.4.6. *The map Ψ is a morphism of groups.*

Proof. Clearly the morphism π sends $\mathbf{G}_{L^\star}$ into $\mathbf{Q}_{L^\star}$, and

$$\begin{tikzcd}
\mathbf{G}_{L^\star} \arrow[r, "\varepsilon"] \arrow[d, "\pi"] & E \arrow[r] & E/\Lambda \arrow[d] \\
\mathbf{Q}_{L^\star} \arrow[rr, "\Psi"] & & E/(F + \Lambda)
\end{tikzcd}$$

is commutative, where both the right column and the right arrow in the top row are the canonical projections. Now let us denote by Φ the map given by composition of the top row of the diagram. According to Section 1.9, the image of the rational points of $\mathbf{G}$ through π is the whole group of the rational points of $\mathbf{Q}$. It follows that the left column of the diagram is an epimorphism of groups. Thus in order to prove that Ψ is a group morphism it is enough to show that Φ is. To this end, let $f, g \in \mathbf{G}_{L^\star}$. They are automorphisms of V, acting as the identity on V_1, normalizing V_{m-1} and acting as the identity on V/V_{m-1}. Also, $V_{m-1} \cap L$ and $V_1 + L$ are stable under them. Now let $y \in L$. Clearly, $g(y) - y$ lies in $V_{m-1} \cap (V_1 + L)$, which is equal to $V_1 + (V_{m-1} \cap L)$ by Dedekind's modular law. Then it follows easily that

$$h(g(y) - y) - (g(y) - y) \in V_{m-1} \cap L,$$

which in turn shows that

$$h \circ g(y) - g(y) - h(y) \in L.$$

Finally, since the projection p of V onto V_1 along V_1' sends L into $V_1 \cap L$, we obtain that

$$p \circ h \circ g(y) - p \circ g(y) - p \circ h(y) \in V_1 \cap L,$$

and the thesis follows. □

Now let us denote by K the kernel of Ψ. Then

Proposition 3.4.7. *For any rational point g of $\mathbf{G}$ such that $\pi(g)$ is in K, we have that $g \in \mathbf{G}_{L^\star}$ and that $\varepsilon(g) \in F + \Lambda$.*

Proof. Clearly

$$\begin{array}{ccc} \mathbf{G}_{L^\star} & \xrightarrow{\varepsilon} & E \\ \downarrow{\scriptstyle\pi} & & \downarrow \\ \mathbf{Q}_{L^\star} & \xrightarrow{\Psi} & E/(F+\Lambda) \end{array}$$

is commutative, where the right column is the canonical projection. The claim follows immediately from this fact. □

Finally, we can state the main result of this section, that is to say,

Theorem 3.4.1. *The group morphism given by composition of*

$$\mathbf{G}_L \to \mathbf{G}(\mathbb{Q}) \xrightarrow{\pi} \mathbf{Q}(\mathbb{Q}),$$

where the left arrow is the inclusion, has kernel $\mathbf{N}_L$ and image K.

Proof. The only non-trivial part of the statement is the one concerning the image of the morphism. Using Proposition 3.4.4 and the commutativity of

$$\begin{array}{ccc} \mathbf{G}_{L^\star} & \xrightarrow{\varepsilon} & E \\ \downarrow{\scriptstyle\pi} & & \downarrow \\ \mathbf{Q}_{L^\star} & \xrightarrow{\Psi} & E/(F+\Lambda) \end{array}$$

where the right column is the canonical projection, we have that the image is contained in K. To prove the other inclusion, let k be an element in K. Since $\mathbf{G}$ and $\mathbf{Q}$ are unipotent, we know that there exists $g \in \mathbf{G}(\mathbb{Q})$ such that $\pi(g) = q$. Then Proposition 3.4.7 assures that $g \in \mathbf{G}_{L^\star}$ and that there exists $h \in \mathbf{N}(\mathbb{Q})$ such that $\epsilon(g)$ is the sum of $\epsilon(h)$ and of an element in Λ. Of course, $gh^{-1} \in \mathbf{G}_{L^\star}$ and its image through π is again k. Also, by Proposition 3.4.5 we have that $\epsilon(gh^{-1})$ lies in Λ. Finally the thesis follows using Proposition 3.4.4. □

We will also need a strengthened version of the first statement of Proposition 3.4.5. Since E is a finite dimensional vector space, it makes sense to consider the affine algebraic group associated to it, which we denote by $\bullet \otimes E$. Also, for any $\mathbb{Q}$-algebra R, we have that $R \otimes V_1$, $R \otimes V_1'$ and $R \otimes V_{m-1}'$ are submodules of $R \otimes V$, and that the sum of $R \otimes V_1$ and of $R \otimes V_1'$ in $R \otimes V$ is direct and is equal to the whole $R \otimes V$. Also, any element of $\mathbf{N}(R)$ can be regarded as an automorphism of $R \otimes V$. Further, $R \otimes E$ is canonically isomorphic to the module of the R-linear maps from $R \otimes V_{m-1}'$ to $R \otimes V_1$. Altogether, it makes sense to consider the map from $\mathbf{N}(R)$ to $R \otimes E$ sending any automorphism h of $R \otimes V$ contained in $\mathbf{N}(R)$ to the unique element of $R \otimes E$ corresponding to the composition of the restriction of h to $R \otimes V_{m-1}'$ with the projection of $V \otimes R$ onto $V_1 \otimes R$ along the complement $R \otimes V_1'$. Also, it is easy to check that the family of these maps over the $\mathbb{Q}$-algebras gives a natural transformation from $\mathbf{N}$ to $\bullet \otimes E$. Since on the rational points it is precisely ε, we will denote the whole natural transformation with such a symbol, too. Then

Proposition 3.4.8. *We have that ε is a monomorphism of algebraic groups from $\mathbf{N}$ to $\bullet \otimes E$. In particular, F is a subspace of E, and the image of $\mathbf{N}$ through ε is $\bullet \otimes F$.*

Proof. It is enough to prove that ε is a monomorphism of algebraic groups, since the rest of the statement follows then by Lemma 3.3.1. In turn, to this end it suffices to show that for any $\mathbb{Q}$-algebra R the map from $\mathbf{N}(R)$ to $R \otimes E$ is a group monomorphism. This can be done with a straightforward adaptation of the proof of Proposition 3.4.5. □

3.5 The Lie algebra side

Let V be a finite dimensional vector space over $\mathbb{Q}$, $\mathfrak{g}$ a nilpotent sub-Lie-algebra of $\mathfrak{gl}(V)$ consisting of nilpotent endomorphisms, and L is a full-dimensional lattice of V. Also, let

$$0 = V_0 \leq \cdots \leq V_i \leq \cdots \leq V_m = V$$

be a flag for V with respect to the action of $\mathfrak{g}$ corresponding to the inclusion of $\mathfrak{g}$ into $\mathfrak{gl}(V)$, of length al least 2. There exists a unique unipotent algebraic subgroup $\mathbf{G}$ of GL_V such that $\mathfrak{g}$ is the Lie algebra of $\mathbf{G}$ and that the inclusion of $\mathfrak{g}$ into $\mathfrak{gl}(V)$ is the differential of the inclusion of $\mathbf{G}$ into GL_V. In particular, $\mathbf{G}$ acts faithfully on V. Also, it is easy to see that the flag for V with respect to the action of $\mathfrak{g}$ that we have at hand is also a flag with respect to the action of $\mathbf{G}$. Therefore we are in the setting of Section 3.4, and all the constructions and the results contained in it make sense here. In the following, we will make free use of them. Since V_{m-1} is $\mathfrak{g}$-stable, $\mathfrak{g}$ acts on it. Similarly, $\mathfrak{g}$ acts on V/V_1.

It follows that $\mathfrak{g}$ acts on their direct sum, that is to say, on $V^\star$. Let us denote by $\mathfrak{n}$ its kernel. Then, in the notations of Section 3.4,

Proposition 3.5.1. *We have that* $\mathfrak{n}$ *is the unique sub-Lie-algebra of* $\mathfrak{gl}(V)$ *such that* $\mathfrak{n}$ *is the Lie algebra of* $\mathbf{N}$ *and that the inclusion of* $\mathfrak{n}$ *into* $\mathfrak{gl}(V)$ *is the differential of the inclusion of* $\mathbf{N}$ *into* GL_V*.*

Proof. It is easy to see that the action of $\mathfrak{g}$ on $V^\star$ is the differential of the action of $\mathbf{G}$ on $V^\star$. From this, the thesis follows easily. □

In particular, the exponential and logarithmic maps are mutually inverse maps between the rational points of $\mathbf{N}$ and $\mathfrak{n}$. Also, since any element of $\mathfrak{n}$ is an endomorphism of V, it makes sense to consider the linear transformation ξ from $\mathfrak{n}$ to E sending any element of $\mathfrak{n}$ to the composition of its restriction to V'_{m-1} with the projection of V onto V_1 along V'_1. Then

Proposition 3.5.2. *We have that*

$$\begin{tikzcd} \mathbf{N}(\mathbb{Q}) \arrow[r, "\varepsilon"] \arrow[d] & E \\ \mathfrak{n} \arrow[ur, "\xi"'] & \end{tikzcd}$$

is commutative, where the vertical arrow is the logarithmic map.

Proof. Of course ξ can be extended to a map from $\mathfrak{gl}(V)$ to E, again sending any endomorphism of V to the composition of its restriction to V'_{m-1} with the projection of V onto V_1 along V'_1. We still denote by ξ such a new function. Now let us denote by id_V the identity function on V. Also, let $h \in \mathbf{N}(\mathbb{Q})$, and $x \in V$. Since h acts as the identity on V/V_1, we have that $(h - \mathrm{id}_V)(x) \in V_1$. In turn, since h acts as the identity on V_1, we obtain that $(h - \mathrm{id}_V)^2(x) = 0$. Altogether, this shows that

$$\log(h) = h - \mathrm{id}_V.$$

Also, since V'_{m-1} is contained in V'_1, we have that ξ sends id_V to 0. Then the thesis follows easily comparing the definitions of ε and of ξ. □

Let us denote by $\mathfrak{q}$ the image of the action of $\mathfrak{g}$ on $V^\star$, and by $\mathrm{d}\pi$ the epimorphism of Lie algebras from $\mathfrak{g}$ to $\mathfrak{q}$. Of course we can regard $\mathbf{Q}$ as an algebraic subgroup of $\mathrm{GL}_{V^\star}$, and $\mathfrak{q}$ as a sub-Lie-algebra of $\mathfrak{gl}(V^\star)$. Then

Proposition 3.5.3. *We have that* $\mathfrak{q}$ *is a nilpotent Lie algebra consisting of nilpotent endomorphisms, and that*

$$0 = V_0^\star \leq \cdots \leq V_i^\star \leq \cdots \leq V_{m-1}^\star = V^\star$$

is a flag for $V^\star$ *with respect to the action of* $\mathfrak{q}$ *corresponding to the inclusion of* $\mathfrak{q}$ *into* $\mathfrak{gl}(V^\star)$*. Also,* $\mathfrak{q}$ *is the Lie algebra of* $\mathbf{Q}$*, and the inclusion of* $\mathfrak{q}$ *into* $\mathfrak{gl}(V^\star)$ *is the differential of the inclusion of* $\mathbf{Q}$ *into* $\mathrm{GL}_{V^\star}$*. Further,* $\mathrm{d}\pi$ *is the differential of the epimorphism* π *of algebraic groups from* $\mathbf{G}$ *onto* $\mathbf{Q}$*.*

Proof. It is immediate to check that the subspaces of the form $V_i^\star$ for i between 0 and $m-1$ form a flag for the action of $\mathfrak{g}$ on $V^\star$. The proof now is easy. □

3.6 The big picture

Let $\mathbf{G}$ be an affine algebraic group over $\mathbb{Q}$ acting faithfully on a finite dimensional vector space V. Also, let L be a full dimensional lattice of V. Then it makes sense to consider the normalizer $\mathbf{G}_L$ of L with respect to the action of the rational points of $\mathbf{G}$ on V.

Proposition 3.6.1. *If the action of* $\mathbf{G}$ *on* V *admits a flag of length at most* 1*, then* $\mathbf{G}$ *is the trivial algebraic group and* $\mathbf{G}_L$ *is the trivial group.*

Proof. If this is the case, $\mathbf{G}$ acts trivially on V. Since it also acts faithfully on V, the first part of the statement follows. The second part is an easy consequence. □

Also,

Theorem 3.6.1. *We have that* $\mathbf{G}_L$ *is a* T*-group whose Hirsch length is equal to the dimension of* $\mathbf{G}$.

Proof. Any action of a unipotent affine algebraic group over $\mathbb{Q}$ on a finite dimensional vector space admits a flag. In particular, it admits a flag of shortest length. Thus we will procede by induction on the length of a shortest flag. In case this is at most 1, from Proposition 3.6.1 it follows easily that $\mathbf{G}_{L^\star}$ is a T-group and that both the dimension of $\mathbf{G}$ and the Hirsch length of $\mathbf{G}_{L^\star}$ are zero. Now suppose that the length of a shortest flag is $m \geq 2$. Then we are in the setting of Section 3.4. In the following, we will make free use of the constructions and the results in it. In particular, by Proposition 3.4.2 the action of $\mathbf{Q}$ on $V^\star$ admits a flag of length at most $m-1$. Also, the action is faithful and $L^\star$ is a full-dimensional lattice of $V^\star$. Therefore by inductive hypothesis $\mathbf{Q}_{L^\star}$ is a T-group, whose Hirsch length is equal to the dimension of $\mathbf{Q}$. In particular, it is a finitely generated group. By Proposition 3.4.3, $E/(F+\Lambda)$ is a periodic abelian group. Also, by Proposition 3.4.6 we know that Ψ is a group morphism. All together, we deduce that the image of Ψ is a finite group, and therefore that the kernel K is a subgroup of finite index in $\mathbf{Q}_{L^\star}$. Hence it is a T-group of Hirsch length equal to the dimension of $\mathbf{Q}$, too. Also, by Propositions 3.4.4 and 3.4.8, we have that the dimension of $\mathbf{N}$ is equal to the dimension of F, and that $\mathbf{N}_L$ is isomorphic to $F \cap L$. In particular, $\mathbf{N}_L$ is a torsion free abelian group of rank equal to the dimension of $\mathbf{N}$. Therefore by Theorem 3.4.1 we conclude that $\mathbf{G}_L$ is a T-group with Hirsch length equal to the sum of the dimensions of $\mathbf{N}$ and $\mathbf{Q}$, and the thesis follows. □

Now let us denote by S the symmetric algebra on the dual of $\mathrm{End}(V)$. Also, let A be a finitely generated commutative $\mathbb{Q}$-algebra, η a natural isomorphism from $\mathbf{G}$ to $\mathrm{Hom}(A, \bullet)$ and φ a morphism of algebras from S to A forming shadow data for $\mathbf{G}$ and its action on V, and let us suppose that A, η and φ are explicitely given. Let us denote by d the dimension of $\mathbf{G}$. In these hypothesis, we are able to compute a finite set of generators for the kernel of φ. Starting from them, it is well-known how to compute the unique sub-Lie-algebra $\mathfrak{g}$ of $\mathfrak{gl}(V)$ such that $\mathfrak{g}$ is the Lie algebra of $\mathbf{G}$ and that the inclusion of $\mathfrak{g}$ into $\mathfrak{gl}(V)$ is the differential of the monomorphism from $\mathbf{G}$ to GL_V. The action of $\mathfrak{g}$ on V admits a flag. Also, with basic linear algebra techniques it is possible to compute it. Now let us denote by $\mathbf{G}'$ the algebraic subgroup of GL_V given by the image of the monomorphism of algebraic groups from $\mathbf{G}$ to GL_V. Of course, it is the unique algebraic subgroup of GL_V such that $\mathfrak{g}$ is the Lie algebra of $\mathbf{G}$ and that the inclusion of $\mathfrak{g}$ into $\mathfrak{gl}(V)$ is the differential of the inclusion of $\mathbf{G}$ into GL_V. Also, the inclusion of $\mathbf{G}'$ into GL_V corresponds to a faithful action on V. Therefore it makes sense to consider the normalizer $\mathbf{G}'_L$ of L with respect to the action of the rational points of $\mathbf{G}'$ on V. By Theorem 3.6.1, it is a T-group of Hirsch length equal to the dimension of $\mathbf{G}'$, which is precisely d. Therefore it admits a T-sequence of length d, let us say $g'_1, \ldots, g'_d$. Now suppose we were able to compute it. Since any of the g'_i is an endomorphism of V that lies in the image of $\mathbf{G}(\mathbb{Q})$ in $\mathrm{End}(V)$ through the natural transformation from $\mathbf{G}$ to $\bullet \otimes \mathrm{End}(V)$, in our hypothesis we are able to compute g_i in $\mathbf{G}(\mathbb{Q})$ whose image in $\mathrm{End}(V)$ is g'_i. Needless to say, $g_1, \ldots, g_d$ is a T-sequence for $\mathbf{G}_L$.

Therefore it remains to show that, given a nilpotent sub-Lie-algebra $\mathfrak{g}$ of $\mathfrak{gl}(V)$ consisting of nilpotent endomorphisms together with a flag

$$0 = V_0 \leq \cdots \leq V_i \leq \cdots \leq V_m = V$$

for the corresponding action of $\mathfrak{g}$ on V, we are able to compute a T-sequence for the normalizer $\mathbf{G}_L$ of L with respect to the action of $\mathbf{G}$ on V, where now $\mathbf{G}$ denotes the unique algebraic subgroup of GL_V such that $\mathfrak{g}$ is the Lie algebra of $\mathbf{G}$ and the inclusion of $\mathfrak{g}$ into $\mathfrak{gl}(V)$ is the differential of the inclusion of $\mathbf{G}$ into GL_V, and the action of $\mathbf{G}$ on V is the one corresponding to the inclusion of $\mathbf{G}$ into GL_V. Recall that the flag we are given is also a flag for the action of $\mathbf{G}$ on V. Then, if the length m of the flag is less or equal to 1, then Proposition 3.6.1 assures that the empty set is a T-sequence for $\mathbf{G}_L$. Now suppose that $m \geq 2$. Therefore we are in the setting of Section 3.5, and we will use freely notations and results in it. Also, since the case for $m \leq 1$ has already been settled, we can assume inductively that we are able to solve the problem whenever the given flag has length strictly smaller that m. As a first thing, note that it is easy to compute the vector space $V^\star$, its subspaces $V_i^\star$ for i between 0 and $m-1$, and its lattice $L^\star$. Also, the sub-Lie-algebra $\mathfrak{q}$ of $\mathfrak{gl}(V^\star)$ which is the image of the action of $\mathfrak{g}$ on $V^\star$ and the epimorphism $\mathrm{d}\pi$ of Lie algebras from $\mathfrak{g}$ onto $\mathfrak{q}$ are easily computed. In fact, these computations rely upon just basic linear algebra techniques. Then Proposition 3.5.3 and the inductive hypothesis guarantee that we are able to compute a T-sequence for $\mathbf{Q}_{L^\star}$. Let us denote it by $q_1, \ldots, q_c$. Further, the discussion at the end of Section 3.1 assures that we are able to compute the subspaces V'_1 and V'_{m-1} of V. Since the discussion shows that we are even able to compute a basis of the free abelian groups $V'_1 \cap L$ and $V'_{m-1} \cap L$, the proof of Proposition 3.4.3 shows that computing E and a basis of Λ inside it is straightforward, too. Proposition 3.5.2 shows that F is equal to the image of ξ. Therefore computing a basis for F is just linear algebra. Also, the image through π of the exponential g'_i of any element in $\mathfrak{g}$ whose image through $\mathrm{d}\pi$ is the logarithm of q_i, is precisely q_i. Of course, such a g'_i is easily computed since $\mathrm{d}\pi$ is a surjective linear transformation. With these data at hand, it is not hard to compute the basis in Hermite normal form for the relation lattice of $\Psi(q_1), \ldots, \Psi(q_c)$. With these ingredients at hand, the discussion at the end of Section 3.2 shows how to compute a T-sequence for K. We already know that it will consist of c elements. Let us denote them by $k_1, \ldots, k_c$. For any of the k_i, let us denote by g''_i any element of $\mathbf{G}(\mathbb{Q})$ whose image through π is k_i. Of course it can be easily computed in the same way we computed g'_i beginning from q_i. Also, we know by Proposition 3.4.7 that $\varepsilon(k_i)$ is the sum of an element in Λ and an element $f_i \in F$. Of course such an f_i is easily computed, as well as it is easy to find a element n_i in $\mathbf{N}(\mathbb{Q})$ whose image through ε is precisely f_i. In fact, by virtue of Proposition 3.5.2 it is enough to take the exponential of any element in $\mathfrak{n}$ whose image through ξ is precisely f_i. Finally, combining Propositions 3.4.5 and 3.4.4, we conclude that $g_i = g_i'' n_i^{-1}$ lies in G_L and that their images through π form a T-sequence for K. Finally let $h_1, \ldots, h_b$ be the images through the exponential map of some $y_1, \ldots, y_b$ in $\mathfrak{n}$ whose images through ξ form a basis for $F \cap \Lambda$. Again by Propositions 3.5.2 and 3.4.4, we deduce that $h_1, \ldots, h_b$ is a T-sequence for $\mathbf{N}_L$. Of course, it is easy to compute. Finally, by virtue of Theorem 3.4.1 we have that $g_1, \ldots, g_c, h_1, \ldots, h_b$ is a T-sequence for $\mathbf{G}_L$.

3.7 Numerical experiences

Let us denote by $\mathbf{G}$ the subfunctor of GL_4 that to any $\mathbb{Q}$-algebra R associates

$$\mathbf{G}(R) = \left\{ \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & \frac{1}{2}c^2 \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_4(R) \text{ such that } a, b, c \in R \right\}.$$

It is easy to check that it is an affine algebraic subgroup of GL_4 over $\mathbb{Q}$. Indeed, let us denote by $\mathbb{Q}[\hat{X}]$ the polynomial algebra with rational coefficients in the indeterminates X_{ij} for i and j between 1 and 4, by $\mathfrak{a}$ its ideal generated by $X_{ii} - 1$ for i between 1 and 4, X_{ij} for $1 \leq j < i \leq 4$, X_{12}, $X_{23} - X_{34}$ and $2X_{24} - X_{23}X_{34}$, and let us put $A = \mathbb{Q}[\hat{X}]/\mathfrak{a}$. Then A is finitely generated, and there exists a natural isomorphism η from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$ that to every $\mathbb{Q}$-algebra R associates

$$\mathrm{Hom}(A, R) \to \mathbf{G}(R) \quad , \quad f \mapsto \begin{pmatrix} f(X_{11}) & f(X_{12}) & f(X_{13}) & f(X_{14}) \\ f(X_{21}) & f(X_{22}) & f(X_{23}) & f(X_{24}) \\ f(X_{31}) & f(X_{32}) & f(X_{33}) & f(X_{34}) \\ f(X_{41}) & f(X_{42}) & f(X_{43}) & f(X_{44}) \end{pmatrix}.$$

In particular, we have at hand the canonical action of $\mathbf{G}$ on $\mathbb{Q}^4$. For short, we will denote $\mathbb{Q}^4$ also by V. Also, $\mathbb{Z}^4$ is a full-dimensional lattice of $\mathbb{Q}^4$. We will denote it by L, too. Further, let us denote by S the symmetric algebra on the dual of $\mathrm{End}(V)$, and by φ the map given by composition of

$$S \to \mathbb{Q}[\hat{X}] \to A,$$

where the arrow on the left is the isomorphism with respect to the canonical basis of V, and the arrow on the right is the canonical projection. Then it is easy to see that A, η and φ are shadow data for $\mathbf{G}$ and its action on V. Of course, they are explicitely given. Therefore we are in the hypothesis of Section 3.6. We will now apply the algorithm described in it. As a first thing, it is easy to see that $\mathfrak{g}$ is the sub-Lie-algebra of $\mathfrak{gl}(V)$ with basis consisting of the endomorphisms x_1, x_2 and x_3 whose matrices with respect to the canonical basis of V are

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Now let us denote by e_1, e_2, e_3, e_4 the canonical basis of $\mathbb{Q}^4$. Then a flag for the action of $\mathfrak{g}$ on $\mathbb{Q}^4$ is given by

$$0 = V_0 < V_1 < V_2 < V_3 = V \ ,$$

where V_1 is the subspace generated by e_1 and e_2, and V_2 is generated by e_1, e_2 and e_3. Since its length is 3, we have to apply the non-trivial part of the algorithm. From now on we will use the notations of the last paragraph of Section 3.6. As a first thing, note that $L^\star$ has basis given by $e_1^\star = (e_1, 0)$, $e_2^\star = (e_2, 0)$, $e_3^\star = (e_3, 0)$, $e_4^\star = (0, e_3 + V_1)$ and $e_5^\star = (0, e_4 + V_1)$, which is therefore also a basis for $V^\star$. Also, $V_1^\star$ is generated by $e_1^\star$, $e_2^\star$ and $e_4^\star$. A basis for the sub-Lie-algebra $\mathfrak{q}$ of $\mathfrak{gl}_{V^\star}$ is given by the endomorphisms y_1 and y_2 of $V^\star$ whose matrices with respect to $e_1^\star, e_2^\star, e_3^\star, e_4^\star, e_5^\star$ are

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} .$$

Further, $\mathrm{d}\pi$ sends x_1 to y_1, x_2 to the zero endomorphism of $V^\star$, and x_3 to y_2. Applying the algorithm recursively to $\mathfrak{q}$, $V^\star$ and the previously computed flag we find that the endomorphisms q_1 and q_2 of $V^\star$, whose matrices are

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} ,$$

are a T-sequence for $\mathbf{Q}_{L^\star}$. Also, we can take as V_1' the subspace of V generated by e_3 and e_4, and by V_2' the subspace generated by e_4. Of course, e_3 and e_4 are also a basis for $V_1' \cap L$, and e_4 is also a basis for $V_2' \cap L$. Now let us denote by f_1 the endomorphism in E sending e_4 to e_1 and by f_2 the endomorphism sending e_4 to e_2. Then f_1 and f_2 form a basis for E, as well as a basis for Λ. Also, it is immediate to see that $\mathfrak{n}$ is the sub-Lie-algebra of $\mathfrak{gl}(V)$ generated by x_2. Therefore F is the subspace of E with basis f_1. Also, since both the logarithm of q_1 and the image of x_1 through $\mathrm{d}\pi$ is equal to y_1, we can put $g_1' = \exp(x_1)$. Similarly, we can take $g_2' = \exp(x_3)$. It follows that

$$\Psi(q_1) = 0 \quad \text{and} \quad \Psi(q_2) = \frac{1}{2} f_2 + F + \Lambda.$$

It is easy to see that a basis in Hermite normal form for the relation lattice of $\Psi(q_1)$ and $\Psi(q_2)$ in $E/F + \Lambda$ is given by $(1, 0)$ and $(0, 2)$. Therefore, a T-sequence for K is given by $k_1 = q_1$ and $k_2 = q_2^2$, hence we can put $g_1'' = g_1'$ and $g_2'' = (g_2')^2$. Note that the matrices of g_1'' and of g_2'' are

$$\hat{g}_1'' = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \hat{g}_2'' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} ,$$

respectively. This shows that both $\varepsilon(g_1'')$ and $\varepsilon(g_2'')$ are in Λ. Therefore we can take $g_1 = g_1''$ and $g_2 = g_2''$. Also, a basis for $F \cap \Lambda$ is given by f_1. Hence we can take as h_1 the exponential of x_2, that it to say, the endomorphism with matrix

$$\hat{h}_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

Now let us denote by e_{ij} for i and j between 1 and 4 the unique endomorphism of V sending e_i to e_j and all the other elements of the canonical basis of V to 0. The e_{ij} form a basis for $\mathrm{End}(V)$. Let us denote by e_{ij}^* the elements of the basis of $\mathrm{End}(V)^*$ dual to it. Then through the natural isomorphism between $\mathrm{End}(\bullet \otimes V)$ and $\mathrm{Hom}(S, \bullet)$ with respect to the canonical basis of V, we have that g_1 corresponds to the morphism f from S to $\mathbb{Q}$ sending e_{ii}^* to 1 for every i between 1 and 4, e_{13}^* to 0, and all the other elements of the given basis of S o 0. We know that there exists a morphism f' from A to $\mathbb{Q}$ such that $f = f' \circ \varphi$. More precisely, f' is the endomorphism sending any $X_{ii} + \mathfrak{a}$ to 1 for every i between 1 and 4, $X_{13} + \mathfrak{a}$ to 1, and $X_{ij} + \mathfrak{a}$ to 0 for the remaining suitable choices of the indexes i and j. In turn, such an endomorphism corresponds through η to $\hat{g}_1$. In the very same way, starting from g_2 and h_1, we find $\hat{g}_2$ and $\hat{h}_1$. Therefore $\hat{g}_1$, $\hat{g}_2$ and $\hat{h}_1$ are a T-sequence for G_L, where of course $\mathbf{G}$ now denotes the original algebraic group.

The algorithm described in Section 3.6 has been implement in GAP4, and it has been tested on some non-trivial examples. From the computational point of view, the hardest part is the subalgorithm dealing with nilpotent Lie algebras. Indeed, it turns out that its running time growths roughtly exponentially on the length of the flag. This is due to the fact that, at each step of the recursion, the dimension of V and of E become bigger and bigger. In the worst case, V doubles at each step, while E growth by about a factor of 4. As an example, let n be a positive integer, and let us denote by $e_1, \ldots, e_n$ the canonical basis of $\mathbb{Q}^n$, and by e_{ij} the unique endomorphism of $\mathbb{Q}^n$ sending e_i to e_j , and all the other elements of the canonical basis for $\mathbb{Q}^n$ to 0. Also, let $\mathfrak{g}_n$ be the subspace of $\mathfrak{gl}(\mathbb{Q}^n)$ generated by $e_{1,2}, \ldots, e_{1,n}$ and by

$$\sum_{j=2}^{n-1} e_{j,j+1} .$$

Then $\mathfrak{g}_n$ is nilpotent sub-Lie-algebra of $\mathfrak{gl}(\mathbb{Q}^n)$, and a flag of shortest length for its natural action on $\mathbb{Q}^n$ is given by

$$0 = V_0 < \cdots < V_i < \cdots < V_n = \mathbb{Q}^n ,$$

where

$$V_i = \langle e_1, \ldots, e_i \rangle$$

for every i between 1 and i. In particular, it has length n. Also, as a full-dimensional lattice of $\mathbb{Q}^n$ we take $\mathbb{Z}^n$. The running time of the subalgorithm applied to these data on a 2GHz processor with 1GB of memory for GAP is of about 0.7 seconds when n is equal to 6, and of about 3, 24 and 204 seconds when n is equal to 7, 8 and 9, respectively. However, these running times also show that the whole algorithm is efficient enough to tackle nontrivial examples.

Chapter 4

The case of a torus

In this chapter we provide an algorithm solving the problem described in Chapter 2 in the special case in which the given algebraic group is a torus. The structure of the chapter is similar to that of Chapter 3. In fact, the first three sections are devoted to prove some auxiliary results, which are used in Section 4.4 to provide, on one hand, an independent proof of the theorem 2.2.2 in the special case of the tori, and, on the other hand, to describe the algorithm and to prove its correctness. The last section gives some evidences about the practicality of the algorithm.

4.1 From tori to semisimple algebras

Let V be a finite dimensional $\mathbb{Q}$-vector space, and let us denote by $\bullet \otimes V$ the affine space on V. It is an easy verification that for any subfunctor $\mathbf{S}$ of $\bullet \otimes V$ there exists a minimum subspace W of V with the property that $\mathbf{S}(R) \subseteq R \otimes W$ for any algebra R. We refer to it as the subspace of V generated by $\mathbf{S}$. When $\mathbf{S}$ is representable, the subspace generated by it admits another characterization. In fact,

Proposition 4.1.1. *Let A be a commutative $\mathbb{Q}$-algebra, η a natural isomorphism from* $\mathrm{Hom}(A, \bullet)$ *to* $\mathbf{S}$*, and φ a morphism of $\mathbb{Q}$-algebras from S to B such that*

$$\begin{array}{ccc} \mathrm{Hom}(A, \bullet) & \xrightarrow{\sharp\circ\varphi} & \mathrm{Hom}(S, \bullet) \\ \downarrow{\scriptstyle \eta} & & \downarrow \\ \mathbf{S} & \xrightarrow{\sharp\circ\varphi} & \bullet \otimes V \end{array}$$

where S is the symmetric algebra on the dual of V, the bottom row is the inclusion and the right column is the canonical natural isomorphism, is commutative. Then the subspace of V generated by $\mathbf{S}$ *is the orthogonal of* $\ker\varphi \cap V^*$ *with respect to the canonical bilinear form between V and its dual.*

Proof. Through the canonical natural isomorphism between $\bullet \otimes V$ and $\mathrm{Hom}(S, \bullet)$, $\mathbf{S}$ corresponds to the subfunctor of $\mathrm{Hom}(S, \bullet)$ that to any algebra R associates

$$\{\psi \in \mathrm{Hom}(S, R) \text{ such that } \ker\varphi \subseteq \ker\psi\}.$$

Also, if W is a subspace of V, then $\bullet \otimes W$ corresponds to the subfunctor that to any algebra R associates

$$\{\psi \in \mathrm{Hom}(S, R) \text{ such that } (W^\perp) \subseteq \ker\psi\}.$$

Hence $\mathbf{S}$ is contained in $\bullet \otimes W$ if and only if $(W^\perp) \subseteq \ker\varphi$, which in turn is equivalent to the fact that $W^\perp \subseteq \ker\varphi \cap V^*$, and the thesis follows easily. $\square$

Now let $\mathbf{G}$ be an algebraic subgroup of the multiplicative group $(\bullet \otimes \mathrm{End}(V))^\times$ of $\mathrm{End}(V)$. In particular, it is a subfunctor of $\bullet \otimes \mathrm{End}(V)$. Let us denote by D the subspace of $\mathrm{End}(V)$ generated by $\mathbf{G}$. Then

Theorem 4.1.1. *D is a subalgebra of* $\mathrm{End}(V)$. *If $\mathbf{G}$ is commutative, then D is commutative, too. If $\mathbf{G}$ is even of multiplicative type, D is semisimple.*

Proof. As a first thing, let us point out an elementary result concerning Galois connections and closure operators. That is to say,

Lemma 4.1.1. *Let X and Y be two partially ordered sets, and $f^* : X \to Y$ and $f_* : Y \to X$ be the lower and upper adjoint of a Galois connection, respectively. Also, let cl_X be a closure operator on X and cl_Y a closure operator on Y. Further, suppose that, for every $y \in Y$, if y is closed with respect to cl_Y then $f_*(y)$ is closed with respect to cl_X. Then for every $x \in X$ and $y \in Y$, if $f^*(x) \leq y$ then $f^*(\mathrm{cl}_X(x)) \leq \mathrm{cl}_Y(y)$.*

Proof. In our hypothesis, $f^*(x) \leq \mathrm{cl}_Y(y)$, which is equivalent to $x \leq f_*(\mathrm{cl}_Y(y))$. Since $f_*(\mathrm{cl}_Y(y))$ is closed with respect to cl_X, it follows that $\mathrm{cl}_X(x) \leq f_*(\mathrm{cl}_Y(y))$, which is equivalent to our thesis. $\square$

Next, let us introduce some constructions. Let U, W and Z be finite dimensional $\mathbb{Q}$-vector spaces, and β a bilinear function from $U \times W$ to Z. For any algebra R, let us denote by β_R the map obtained from β extending scalars to R. Also, let $\mathbf{Q}$ and $\mathbf{R}$ be subfunctors of $\bullet \otimes U$ and $\bullet \otimes W$, respectively. Then there exists a subfunctor of $\bullet \otimes Z$ that to any algebra R associates

$$\{\beta_R(x, y) \text{ such that } x \in \mathbf{Q}(R) \text{ and } y \in \mathbf{R}(R)\}.$$

We refer to it as the product of $\mathbf{Q}$ and $\mathbf{R}$ with respect to β. A technical but useful result is the following.

Lemma 4.1.2. *Let $\mathbf{T}$ be a subfunctor of $\bullet \otimes Z$, and let us denote by U' the subspace of U generated by $\mathbf{Q}$ and by Z' the subspace of Z generated by $\mathbf{T}$. If the product of $\mathbf{Q}$ and $\mathbf{R}$ with respect to β is contained in $\mathbf{T}$ and $\mathbf{R}$ is representable, then the product of $\bullet \otimes U'$ and $\mathbf{R}$ with respect to β is contained in $\bullet \otimes Z'$.*

Proof. Let us denote by f^* the function from the set of subfunctors of $\bullet \otimes U$ to the set of subfunctors of $\bullet \otimes Z$ that to any $\mathbf{Q}'$ associates the product of $\mathbf{Q}'$ and $\mathbf{R}$ with respect to β. Also, let us denote by f_* the function from the set of subfunctors of $\bullet \otimes Z$ to the set of subfunctors of $\bullet \otimes U$ that to any $\mathbf{T}'$ associates the subfunctor that in turn to any algebra R associates the set of elements $x \in R \otimes U$ such that

$$\beta_S(\varphi \otimes \mathrm{id}_U(x), y) \in \mathbf{T}'(S)$$

for every algebra S, every morphism of algebras φ from R to S and every $y \in \mathbf{R}(S)$. Recall that both the set of subfunctors of $\bullet \otimes U$ and the set of subfunctors of $\bullet \otimes Z$ are endowed with a partial order given by inclusion. With respect to these orders, it turns out that f^* and f_* are the lower and the upper adjoint of a Galois connection, respectively. Also, the function from the set of subfunctors of $\bullet \otimes U$ to itself that to any $\mathbf{Q}'$ associates $\bullet \otimes U''$, where U'' is the subspace of U generated by $\mathbf{Q}'$, is a closure operator. Of course, the same is true for Z, *mutatis mutandis*. Therefore the thesis will follow from Lemma 4.1.1 once we will have proven that for any subspace Z'' of Z, $f_*(\bullet \otimes Z'')$ is of the form $\bullet \otimes U''$ for some subspace U'' of U.

In order to prove this last claim, let B be a commutative $\mathbb{Q}$-algebra, η a natural isomorphism from $\mathrm{Hom}(B, \bullet)$ to $\mathbf{R}$, and let us denote by w the image of the identity function of B through η. Of course, $w \in B \otimes W$. Also, for every algebra R,

$$\mathrm{Hom}(B, R) \to R \otimes W \ , \quad f \mapsto f \otimes \mathrm{id}_W(w)$$

is injective with image $\mathbf{R}(R)$. Then we have at hand the map given Ψ given by composition of

$$U \overset{1 \otimes \mathrm{id}_U}{\longrightarrow} B \otimes U \to B \otimes Z \to \frac{B \otimes Z}{B \otimes Z''}$$

where the central map sends any $u \in B \otimes U$ to $\beta_B(w, u)$ and the map on the right is the canonical projection. Of course it is a linear transformation, hence its kernel is a subspace of U. We will finish the proof showing that it is the subspace we are searching for.

To this end, let us fix a $\mathbb{Q}$-algebra R. The existence of w gives us a useful criterion to test membership of an element x of $R \otimes U$ to the set of R-valued points of $f_*(\mathbf{T}')$, where $\mathbf{T}'$ is any subfunctor of $\bullet \otimes Z$. In fact, if we denote by i the morphism of algebras from R to $R \otimes B$ sending r to $r \otimes 1$, and by j the morphism from B to $R \otimes B$ sending b to $1 \otimes b$, then we have that $x \in f_*(\mathbf{T}')(R)$ if and only if

$$\beta_{R \otimes B}\big(i \otimes \mathrm{id}_U(x), j \otimes \mathrm{id}_W(w)\big) \in \mathbf{T}'(R \otimes B).$$

It is easy to see that the condition is necessary. Roughly speaking, to show that it is also sufficient we have to exploit the universal property of the tensor product of algebras. Coming back to our problem, let us consider the map Ψ_R given by composition of

$$R \otimes U \overset{i \otimes \mathrm{id}_U}{\longrightarrow} R \otimes B \otimes U \to R \otimes B \otimes Z \to \frac{R \otimes B \otimes Z}{R \otimes B \otimes Z''}$$

where the central map sends any $u \in R \otimes B \otimes U$ to $\beta_{R \otimes B}\big(u, j \otimes \mathrm{id}_W(w)\big)$ and the map on the right is the canonical projection. The previous criterion shows that the kernel of Ψ_R is the set of R-valued points of $f_*(\bullet \otimes Z'')$. Also,

$$\begin{array}{ccc} U & \xrightarrow{\quad\Psi\quad} & B \otimes Z / B \otimes Z'' \\ {\scriptstyle 1 \otimes \mathrm{id}_U}\big\downarrow & & \big\downarrow \\ R \otimes U & \xrightarrow{\quad\Psi_R\quad} & R \otimes B \otimes Z / R \otimes B \otimes Z'' \end{array}$$

is commutative, where the right column is the map given by composition of

$$\frac{B\otimes Z}{B\otimes Z''}\xrightarrow{1\otimes \mathrm{id}} R\otimes\frac{B\otimes Z}{B\otimes Z''}\to\frac{R\otimes B\otimes Z}{R\otimes B\otimes Z''},$$

where in turn the map on the right is the canonical isomorphism. Since the tensor product is left exact, we deduce that the kernel of Ψ_R is $R\otimes\ker\Psi$, and the thesis follows easily. □

The first two claims of the theorem are now easy to prove. Since multiplication of $\mathrm{End}(V)$ is a bilinear map from $\mathrm{End}(V)\times\mathrm{End}(V)$ to $\mathrm{End}(V)$, it makes sense to consider the product of two copies of $\mathbf{G}$ with respect to it. Since $\mathbf{G}$ is an algebraic subgroup of $\big(\bullet\otimes\mathrm{End}(V)\big)^{\times}$, we have that the product is contained in $\mathbf{G}$. Therefore by Lemma 4.1.2 we obtain that the product of $\mathbf{G}$ and $\bullet\otimes D$ is contained in $\bullet\otimes A$, and again by Lemma 4.1.2 that the product of $\bullet\otimes D$ with itself is contained in $\bullet\otimes D$. Taking the groups of the rational points, it follows that D is a subalgebra of $\mathrm{End}(V)$. Now suppose that $\mathbf{G}$ is commutative. Then the product of two copies of $\mathbf{G}$ with respect to the bracket of $\mathrm{End}(V)$ is contained in $\bullet\otimes 0$, and arguing as before we obtain that D is commutative.

In order to complete the proof of the theorem, it is convenient to state another auxiliary result. As before, let U be a finite dimensional vector space, and $\mathbf{Q}$ a subfunctor of $\bullet\otimes U$. Also, let us denote by U' the subspace of U generated by $\mathbf{Q}$. It is easy to check that there exists a unique subfunctor $\widehat{\mathbf{Q}}$ of $\bullet\otimes(\overline{\mathbb{Q}}\otimes U)$ with the property that there exists a natural transformation η from $\mathbf{Q}_{\overline{\mathbb{Q}}}$ to $\widehat{\mathbf{Q}}$ such that

$$\begin{tikzcd}
\mathbf{Q}_{\overline{\mathbb{Q}}} \arrow[r, "\eta"] \arrow[d] & \widehat{\mathbf{Q}} \arrow[d] \\
(\bullet\otimes U)_{\overline{\mathbb{Q}}} \arrow[r] & \bullet\otimes(\overline{\mathbb{Q}}\otimes U)
\end{tikzcd}$$

is commutative, where the columns are the inclusions and the bottow row is the canonical isomorphism, and we have that η is even a natural isomorphism. Also,

Lemma 4.1.3. *The subspace of $\overline{\mathbb{Q}}\otimes U$ generated by $\widehat{\mathbf{Q}}$ is contained in $\overline{\mathbb{Q}}\otimes U'$. If $\mathbf{Q}$ is representable, the other inclusion holds, too.*

Proof. The first inclusion is easily proved since for any $\overline{\mathbb{Q}}$-algebra R the canonical isomorphism between $R\otimes U$ and $R\otimes_{\overline{\mathbb{Q}}}\overline{\mathbb{Q}}\otimes U$ sends $R\otimes U'$ to $R\otimes(\overline{\mathbb{Q}}\otimes U')$.

Now suppose that $\mathbf{Q}$ is representable. As before, there exists a commutative $\mathbb{Q}$-algebra B together with an element $u\in B\otimes U$ such that

$$\mathrm{Hom}(B,R)\to R\otimes U\quad,\quad f\mapsto f\otimes\mathrm{id}_U(u)$$

is an injection with image $\mathbf{Q}(R)$ for every $\mathbb{Q}$-algebra R. Also, it is easy to see that U' is the minimum subspace of U such that $u\in B\otimes U'$. Let us denote by $\overline{u}$ the image of u through the map from $B\otimes U$ into $(\overline{\mathbb{Q}}\otimes B)\otimes_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}\otimes U)$ sending every $b\otimes x$ to $(1\otimes b)\otimes(1\otimes x)$. Again, it is easy to check that for every $\overline{\mathbb{Q}}$-algebra R,

$$\mathrm{Hom}(\overline{\mathbb{Q}}\otimes B,R)\to R\otimes_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}\otimes V)\quad,\quad f\mapsto f\otimes\mathrm{id}_{\overline{\mathbb{Q}}\otimes V}(u)$$

is injective with image $\widehat{\mathbf{Q}}(R)$, and that the subspace of $\overline{\mathbb{Q}} \otimes U$ generated by $\widehat{\mathbf{Q}}$ is the minimum subspace Z of $\overline{\mathbb{Q}} \otimes U$ such that $u \in (\overline{\mathbb{Q}} \otimes B) \otimes_{\overline{\mathbb{Q}}} Z$. Through the canonical isomorphism between $(\overline{\mathbb{Q}} \otimes B) \otimes_{\overline{\mathbb{Q}}} (\overline{\mathbb{Q}} \otimes U)$ and $B \otimes \overline{\mathbb{Q}} \otimes U$, the subspace $(\overline{\mathbb{Q}} \otimes B) \otimes_{\overline{\mathbb{Q}}} Z$ corresponds to $B \otimes Z$. Hence the image of u through the canonical map from $B \otimes U$ to $B \otimes \overline{\mathbb{Q}} \otimes U$ is contained in $B \otimes Z$. Now let us denote by Z' the unique subspace of U such that

$$Z \cap (1 \otimes U) = 1 \otimes Z'.$$

Then $u \in B \otimes Z'$, and therefore $U' \leq Z'$ and $\overline{\mathbb{Q}} \otimes U' \leq \overline{\mathbb{Q}} \otimes Z'$. Now the thesis follows easily. □

Now we are ready to prove the third and last claim. Suppose that $\mathbf{G}$ is of multiplicative type. Of course, it is enough to show that the action of $\overline{\mathbb{Q}} \otimes D$ on $\overline{\mathbb{Q}} \otimes V$ obtained from the natural action of D on V extending scalars to $\overline{\mathbb{Q}}$ is diagonalizable. To this end, note that there exists a unique subfunctor $\widehat{\mathbf{G}}$ of $\bullet \otimes (\overline{\mathbb{Q}} \otimes \mathrm{End}(V))$ – regarded as a functor to the category of sets – with the propery that there exists a natural transformation η from $\mathbf{G}_{\overline{\mathbb{Q}}}$ to $\widehat{\mathbf{G}}$ such that

$$\begin{tikzcd} \mathbf{G}_{\overline{\mathbb{Q}}} \arrow[r, "\eta"] \arrow[d] & \widehat{\mathbf{G}} \arrow[d] \\ (\bullet \otimes \mathrm{End}(V))_{\overline{\mathbb{Q}}} \arrow[r] & \bullet \otimes (\overline{\mathbb{Q}} \otimes \mathrm{End}(V)) \end{tikzcd}$$

is commutative, where the columns are the inclusions and the bottom row is the canonical isomorphism. Also, η is a natural isomorphism. Therefore there exists a unique way to endow $\widehat{\mathbf{G}}$ with the structure of affine algebraic group over $\mathbb{Q}$ in such a way that η becomes an isomorphism of affine algebraic groups over $\overline{\mathbb{Q}}$, and in this way we have that $\widehat{\mathbf{G}}$ is even an algebraic subgroup of $(\bullet \otimes \overline{\mathbb{Q}} \otimes \mathrm{End}(V))^{\times}$. Therefore we have at hand the action of $\widehat{\mathbf{G}}$ on $\overline{\mathbb{Q}} \otimes V$ corresponding to the morphism given by composition of

$$\widehat{\mathbf{G}} \to (\bullet \otimes \overline{\mathbb{Q}} \otimes \mathrm{End}(V))^{\times} \to (\bullet \otimes \mathrm{End}(\overline{\mathbb{Q}} \otimes V))^{\times} \to \mathrm{GL}_{\overline{\mathbb{Q}} \otimes V},$$

where the arrow on the left is the inclusion, the central arrow is the morphism associated to the canonical isomorphism between $\overline{\mathbb{Q}} \otimes \mathrm{End}(V)$ and $\mathrm{End}(\overline{\mathbb{Q}} \otimes V)$, and the arrow on the right is the canonical isomorphism. It is easy to check that if a subspace L of $\overline{\mathbb{Q}} \otimes \mathrm{End}(V)$ is stable under the action of $\widehat{\mathbf{G}}$, then the product of $\widehat{\mathbf{G}}$ and $\bullet \otimes L$ with respect to the bilinear map from the cartesian product of $\overline{\mathbb{Q}} \otimes \mathrm{End}(V)$ and $\overline{\mathbb{Q}} \otimes V$ to $\overline{\mathbb{Q}} \otimes V$, which in turn is obtained from the natural action of $\mathrm{End}(V)$ on V extending scalars to $\overline{\mathbb{Q}}$, is contained in $\bullet \otimes L$. Therefore, if this is the case, by Lemmas 4.1.2 and 4.1.3, we have that L is stable under the action of $\overline{\mathbb{Q}} \otimes D$ on $\overline{\mathbb{Q}} \otimes V$. Since $\widehat{\mathbf{G}}$ is diagonalizable, the thesis follows. □

Let S now denote the symmetric algebra on the dual of $\mathrm{End}(V)$, and let us denote by $x_1, \ldots, x_m$ a basis of V, and by $\mathbb{Q}[\hat{X}]$ the polynomial algebra with rational coefficients in the indeterminates X_{ij} for i and j between 1 and m. Also, let A be a finitely generated commutative $\mathbb{Q}$-algebra, η a natural isomorphism from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$ and φ a morphism from S to A which are shadows data for $\mathbf{G}$ and its action on V corresponding to

$$\mathbf{G} \to (\bullet \otimes \mathrm{End}(V))^{\times} \to \mathrm{GL}_V,$$

where the left arrow is the inclusion and the right arrow is the canonical natural isomorphism. Also, let $f_1, \ldots, f_n$ be a finite set of generators for the kernel of φ. Then Proposition 4.1.1 gives us a recipe to compute D. As a first thing, we have to compute a Grobner basis with respect to a graded ordering for the ideal generated by the images of $f_1, \ldots, f_n$ through the isomorphism between S and $\mathbb{Q}[\hat{X}]$ with respect to $x_1, \ldots, x_m$, and to take the homogeneous polynomials of first degree $h_1, \ldots, h_l$ in it. It is easy to check that the images of $h_1, \ldots, h_l$ through the isomorphism between S and $\mathbb{Q}[\hat{X}]$ are a generating set for $\ker\varphi \cap \mathrm{End}(V)^*$. At this point, it just remains to compute its orthogonal.

4.2 A problem about semisimple algebras

Let D be a finite dimensional, commutative and semisimple $\mathbb{Q}$-algebra, acting faithfully on a finite dimensional $\mathbb{Q}$-vector space V. Also, let L be a full-dimensional lattice of V. The group of units $D^\times$ of D acts on V, hence it makes sense to consider the normalizer $D_L^\times$ of L with respect to this action. Also, let us denote by $E_1, \ldots, E_m$ the decomposition of D in simple ideals, and by $e_1, \ldots, e_m$ the decomposition of the identity corresponding to it. Also, let us denote by V_i the image of V through e_i, by L_i the image of L through e_i, by $\mathcal{O}_i$ the normalizer of L_i with respect to the induced action of E_i on V_i, and by $\mathcal{O}_i^\times$ the group of units of $\mathcal{O}_i$. Then

Proposition 4.2.1. *We have that*

- *the $\mathcal{O}_i$ are orders of the E_i, and that*
- *the image of the cartesian product of the $\mathcal{O}_i^\times$ through the canonical isomorphism from $E_1 \times \cdots \times E_m$ to D is the normalizer $D_{L_1+\cdots+L_m}^\times$ of $L_1 + \cdots + L_m$ with respect to the action of $D^\times$ on V.*

Proof. Of course $\mathcal{O}_i$ acts on L, and the action is faithful since the action of E_i on V_i is. Therefore for any $\alpha \in \mathcal{O}_i$ we have that L is a faithful module over the subring of $\mathcal{O}_i$ generated by α. Since it is also a finitely generated $\mathbb{Z}$-module, we have that α is integral in E_i. Now let $\alpha \in E_i$. Then $\frac{\alpha.L+L}{L}$ is a finitely generated subgroup of $\frac{V}{L}$, which is a periodic group. Therefore there exists an integer n such that $n(\alpha.L) \subseteq L$. Thus the first part of the statement follows easily. In order to prove the second part, note that $\mathcal{O}_i^\times$ is the normalizer of L_i with respect to the action of E_i on V_i, and that the canonical isomorphism ι from $V_1 \oplus \cdots \oplus V_m$ to V sends $L_1 \oplus \cdots \oplus L_m$ to $L_1 + \cdots + L_m$. Therefore the thesis follows from the commutativity of

$$\begin{tikzcd}
\prod_{i=1}^m E_i \times \oplus_{i=1}^m V_i \arrow[r] \arrow[d, "\varphi\times\iota"'] & \oplus_{i=1}^m V_i \arrow[d, "\iota"] \\
D \times V \arrow[r] & V
\end{tikzcd}$$

where φ is the canonical isomorphism from $E_1 \times \cdots \times E_m$ to D. □

Of course there exists a unique action of $D_{L_1+\cdots+L_m}^\times$ on the set of subgroups of $L_1 + \cdots + L_m$ that to any couple (a, H) associates the image $a.H$ of $\{a\} \times H$ through the action of D on V. Also, L is a subgroup of $L_1 + \cdots + L_m$, and

Proposition 4.2.2. *With respect to the action of $D^{\times}_{L_1+\cdots+L_m}$ on the subgroups of $L_1+\cdots+L_m$, the orbit of L is finite, and the stabilizer of L is $D^{\times}_L$.*

Proof. Since L and $L_1+\cdots+L_m$ are both full-dimensional lattices of V, it follows that L has finite index in $L_1+\cdots+L_m$. Also, if a is an element of $D^{\times}_{L_1+\cdots+L_m}$ and H is a subgroup of $L_1+\cdots+L_m$ of finite index, then $a.H$ is of finite index, too, and the two indexes are the same. Since there are only finitely many subgroups of $L_1+\cdots+L_m$ of given finite index, it follows that the orbit of L is finite. Finally, it is easy to see that if $a \in D$ is such that $a.L = L$, then $a.L_i = L_i$. Therefore $D^{\times}_L$ is contained in $D^{\times}_{L_1+\cdots+L_m}$, and the third statement holds, too. □

In particular,

Corollary 4.2.1. *We have that $D^{\times}_L$ is finitely generated.*

Proof. As a consequence of Dirichlet's unit theorem, we know that the group of units of an order of number field is finitely generated. Therefore by Proposition 4.2.1 we have that $D^{\times}_{L_1+\cdots+L_m}$ is finitely generated, too. Then the thesis follows by Proposition 4.2.2. □

Also, we are able to compute a finite set of generators for $D^{\times}_L$. In fact, we have at hand algorithms for computing $E_1, \ldots, E_m$ and $e_1, \ldots, e_m$. Once this has been done, it is easy to compute V_i, its lattice L_i, the action of E_i on V_i, and therefore $\mathcal{O}_i$. Further, using the algorithm due to Posht and Zassenhaus, we obtain finite sets of generators for the $\mathcal{O}^{\times}_i$. With these data at hand, it is easy to compute a finite set of generators for $D^{\times}_{L_1+\cdots+L_m}$. Finally, using the finite orbit stabilizer algorithm, we obtain the finite set of generators we are seaching for.

4.3 Isolating subgroups through characters

Let D be a finite dimensional commutative and semisimple $\mathbb{Q}$-algebra, and $\mathbf{G}$ a connected algebraic subgroup of $(\bullet \otimes D)^{\times}$. Also, let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and let us denote by Γ the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$, by X the set of morphisms from D to $\overline{\mathbb{Q}}$, and by $\mathbb{Z}[X]$ the free abelian group on X. With respect to the standard structure of Γ-module of $\mathbb{Z}[X]$, there exists a unique sub-Γ-module K of $\mathbb{Z}[X]$ such that there exists an isomorphism η from $\mathrm{Hom}(\mathbb{Z}[X]/K, (\bullet \otimes \overline{\mathbb{Q}})^{\times})$ to $\mathbf{G}$ with the property that

$$\begin{tikzcd}
\mathrm{Hom}(\mathbb{Z}[X]/K, (\bullet \otimes \overline{\mathbb{Q}})^{\times}) \arrow[r, "\sharp\circ\pi"] \arrow[d, "\eta"] & \mathrm{Hom}(\mathbb{Z}[X], (\bullet \otimes \overline{\mathbb{Q}})^{\times}) \arrow[d] \\
\mathbf{G} \arrow[r] & (\bullet \otimes D)^{\times}
\end{tikzcd}$$

is commutative, where π is the canonical projection of $\mathbb{Z}[X]$ onto $\mathbb{Z}[X]/K$, the bottom row is the inclusion and the right column is the canonical isomorphism. Of course η is unique, too. Also, let $k_1, \ldots, k_m$ be a finite set of generators for K, regarded as a Γ-module.

Proposition 4.3.1. *For every i between 1 and m, let us denote by Γ_{k_i} the stabilizer of k_i in Γ, and by F_i the subfield of $\overline{\mathbb{Q}}$ consisting of the elements fixed by Γ_{k_i}. Then there exist morphisms of groups φ_i from $D^\times$ to $F_i^\times$ sending $a \in D^\times$ to*

$$\prod_{x \in X} x(a)^{z_x^{(i)}},$$

where $k_i = \sum_{x \in X} z_x^{(i)} x$. Further, we have that

$$\mathbf{G}(\mathbb{Q}) = \bigcap_{i=1}^{m} \ker \varphi_i.$$

Proof. For every i between 1 and m, let us denote by X_i the set of morphisms from F_i to $\overline{\mathbb{Q}}$, by ι_i the inclusion of F_i into $\overline{\mathbb{Q}}$, and by $\mathbb{Z}[X_i]$ the free abelian group with basis X_i. Using Galois theory we have that, with respect to its standard structure of Γ-module, $\mathbb{Z}[X_i]$ is cyclic with generator ι_i, and that the stabilizer of ι_i in Γ is Γ_{k_i}. Therefore there exists a unique morphism ψ_i of Γ-modules from $\mathbb{Z}[X_i]$ to $\mathbb{Z}[X]$ sending ι_i to k_i. In turn, there exists a unique morphism Φ_i of algebraic groups from $(\bullet \otimes D)^\times$ to $(\bullet \otimes F_i)^\times$ such that

$$\begin{tikzcd}
\mathrm{Hom}(\mathbb{Z}[X], (\bullet \otimes \overline{\mathbb{Q}})^\times) \arrow[r, "\sharp \circ \psi_i"] \arrow[d] & \mathrm{Hom}(\mathbb{Z}[X_i], (\bullet \otimes \overline{\mathbb{Q}})^\times) \arrow[d] \\
(\bullet \otimes D)^\times \arrow[r, "\Phi_i"] & (\bullet \otimes F_i)^\times
\end{tikzcd}$$

is commutative, where the columns are the canonical isomorphisms. It is easy to check that φ_i is the map that Φ_i associates to $\mathbb{Q}$. Therefore it is enough to show that $\mathbf{G}$ is the intersection of the kernels of the Φ_i. Now let us denote by $\prod_{i=1}^m (\bullet \otimes F_i)^\times$ the cartesian product of the $(\bullet \otimes F_i)^\times$, and by $\prod_{i=1}^m \Phi_i$ the cartesian product of the Φ_i. Then we can equivalently show that $\mathbf{G}$ is the kernel of $\prod_{i=1}^m \Phi_i$. To this end, let us denote by $\oplus_{i=1}^m \mathbb{Z}[X_i]$ the direct sum of the $\mathbb{Z}[X_i]$ and by $\oplus_{i=1}^m \psi_i$ the direct sum of the ψ_i. As a first thing, it is easy to check that

$$\begin{tikzcd}
\mathrm{Hom}(\mathbb{Z}[X], (\bullet \otimes \overline{\mathbb{Q}})^\times) \arrow[r, "\sharp \circ \oplus_{i=1}^m \psi_i"] \arrow[d] & \mathrm{Hom}(\oplus_{i=1}^m \mathbb{Z}[X_i], (\bullet \otimes \overline{\mathbb{Q}})^\times) \arrow[d] \\
(\bullet \otimes D)^\times \arrow[r, "\prod_{i=1}^m \Phi_i"] & \prod_{i=1}^m (\bullet \otimes F_i)^\times
\end{tikzcd}$$

is commutative, where the right column is the isomorphism given by composition of

$$\mathrm{Hom}(\oplus_{i=1}^m \mathbb{Z}[X_i], (\bullet \otimes \overline{\mathbb{Q}})^\times) \to \prod_{i=1}^m \mathrm{Hom}(\mathbb{Z}[X_i], (\bullet \otimes \overline{\mathbb{Q}})^\times) \to \prod_{i=1}^m (\bullet \otimes F_i)^\times,$$

where the arrow on the left is the canonical isomorphism, and the map on the right is the cartesian product of the canonical isomorphisms from $\mathrm{Hom}(\mathbb{Z}[X_i], (\bullet \otimes \overline{\mathbb{Q}})^\times)$ to $(\bullet \otimes F_i)^\times$. Secondly we have that, regarded as arrows in the category of Γ-modules, π is a cokernel of $\oplus_{i=1}^m \psi_i$, hence $\sharp \circ \pi$ is a kernel of $\sharp \circ \oplus_{i=1}^m$, regarded as arrows in the category of affine algebraic groups. Finally the thesis follows easily combining these two facts. $\square$

Now let us denote by F the splitting field of D inside $\overline{\mathbb{Q}}$, and by G the Galois group of $F/\mathbb{Q}$. Then the image of every morphism in X is contained in F. Also, with respect to the standard product of G-module of $\mathbb{Z}[X]$, we have that K is a sub-G-module of $\mathbb{Z}[X]$, and that a subset of K is a set of generators of K as a Γ-module if and only if it is a set of generators for K as a G-module. Further, for every i between 1 and m, F_i is the subfield of F consisting of the elements fixed by the stabilizer of k_i in G.

In addition, let us denote by S the symmetric algebra on the dual D^* of D, and let A be a finitely generated commutative $\mathbb{Q}$-algebra, φ a morphism from S to A and ζ a natural isomorphism from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$ such that

$$\begin{tikzcd} \mathrm{Hom}(A,\bullet) \arrow[r, "\sharp\circ\varphi"] \arrow[d, "\zeta"] & \mathrm{Hom}(S,\bullet) \arrow[d] \\ \mathbf{G} \arrow[r] & \bullet\otimes D \end{tikzcd}$$

is commutative, where the bottom row is the inclusion and the right column is the canonical isomorphism. Also, let us denote by ι the morphism from S to $\mathbb{Q}$ corresponding to the identity of D through the canonical isomorphism between $\mathrm{Hom}(S, \bullet)$ and $\bullet \otimes D$, by δ the canonical universal ι-differential of S with codomain D^*, and by L the image of the kernel of φ through δ, which is of course a subspace of D^*. Further, let $a_1, \ldots, a_n$ be a basis of D and let us denote by $a_1^*, \ldots, a_n^*$ the basis of D^* dual to it. Then

Proposition 4.3.2. *We have that K is the kernel of the map given by composition of*

$$\mathbb{Z}[X] \to D^* \otimes F \to \frac{D^*}{L} \otimes F,$$

where the arrow on the left is the unique group morphism sending any $x \in X$ to $\sum_{i=1}^n a_i^* \otimes x(a_i)$, and the arrow on the right is the map obtained from the canonical projection of D^* onto D^*/L extending scalars to F.

Proof. We need to introduce some technical constructions first. To this end, let k be a field, $k[\varepsilon]$ a k-algebra generated by an element ε such that $\varepsilon^2 = 0$, and let us denote by $k[\varepsilon]^\times$ its group of units. Also, let M be a finitely generated torsion-free abelian group, and let $\mathbf{G}$ and η be for the moment an affine algebraic group over k and an isomorphism of algebraic groups between $\mathrm{Hom}(M, \bullet^\times)$ and $\mathbf{G}$, respectively. Further, let V denote the tangent space of $\mathbf{G}$, and $\mathrm{Hom}(M, k)$ the k-vector space of group morphisms from M to the additive group of k. Then the map from $\mathrm{Hom}(M, k)$ to V sending any morphism f to the image of

$$M \to k[\varepsilon]^\times \qquad x \mapsto 1 + f(x)\varepsilon$$

through η, is an isomorphism of k-vector spaces. Composing the dual of its inverse with the unique linear transformation from $M \otimes k$ to the dual of $\mathrm{Hom}(M, k)$ sending any $x \otimes a$ to the linear form sending any λ in $\mathrm{Hom}(M, k)$ to $a\lambda(x)$ we obtain a morphism from $M \otimes k$ to the dual V^* of V, which is an isomorphism since the map from $M \otimes k$ to the dual of $\mathrm{Hom}(M, k)$ is. Finally, composing it with the group morphism from M to $M \otimes k$ sending x to $x \otimes 1$ we obtain a group morphism from M to V^*. Since M is torsion-free, the map from M to $M \otimes k$ is injective, hence the whole map from M to V^* is. We will refer to it as the morphism associated to η. Also, let N be another finitely generated torsion-free abelian group, $\mathbf{H}$ an affine algebraic group over k, η' an isomorphism between $\mathrm{Hom}(N,\bullet^{\times})$ and $\mathbf{H}$, f be a morphism from $\mathbf{G}$ to $\mathbf{H}$ and φ a morphism from N to M such that

$$\begin{tikzcd}
\mathrm{Hom}(M,\bullet^{\times}) \arrow[r, "\sharp\circ\varphi"] \arrow[d, "\eta"] & \mathrm{Hom}(N,\bullet^{\times}) \arrow[d, "\eta'"] \\
\mathbf{G} \arrow[r, "f"] & \mathbf{H}
\end{tikzcd}$$

is commutative. Then it is easy to check that

$$\begin{tikzcd}
N \arrow[r, "\varphi"] \arrow[d] & M \arrow[d] \\
W^* \arrow[r] & V^*
\end{tikzcd}$$

is commutative, too, where W^* is the dual of the tangent space of $\mathbf{H}$, the bottom row is the dual of the linear transformation from the tangent space of $\mathbf{G}$ to the tangent space of $\mathbf{H}$ associated to f, and the left and right columns are the morphisms associated to η' and η, respectively. Now let D be for the moment a finite dimensional k-algebra, and let W denote the tangent space of $(\bullet\otimes D)^{\times}$. Then it is easy to check that

$$D \to W \qquad a \mapsto 1+\varepsilon\otimes d$$

is an isomorphism of k-vector spaces. We will refer to it as the canonical isomorphism. In addition, let A be for now be a finitely generated commutative k-algebra, and let $\mathrm{Hom}(A,\bullet)$ be endowed with a structure of affine algebraic group. Also, let η now be a morphism from $\mathrm{Hom}(A,\bullet)$ to $(\bullet\otimes D)^{\times}$, let S denote the symmetric algebra on the dual D^* of D, and let φ be a morphism from S to A such that

$$\begin{tikzcd}
\mathrm{Hom}(A,\bullet) \arrow[r, "\sharp\circ\varphi"] \arrow[d, "\eta"] & \mathrm{Hom}(S,\bullet) \arrow[d] \\
(\bullet\otimes D)^{\times} \arrow[r] & \bullet\otimes D
\end{tikzcd}$$

is commutative, where the bottom row is the inclusion and the right column is the canonical isomorphism. Further, let ι now denote the identity of $\mathrm{Hom}(A,k)$, let δ be a universal ι-differential of A with codomain Ω_A, and let $\mathrm{d}\varphi$ denote the unique linear transformation from D^* to Ω_A such that

$$\begin{tikzcd}
S \arrow[r, "\varphi"] \arrow[d] & A \arrow[d, "\delta"] \\
D^* \arrow[r, "\mathrm{d}\varphi"] & \Omega_A
\end{tikzcd}$$

is commutative, where the left column is the canonical universal $\iota\circ\varphi$-differential of S with codomain D^*. Then it is easy to check that

$$\begin{tikzcd} V \arrow[r] \arrow[d] & W \arrow[d] \\ \Omega_A^* \arrow[r] & D \end{tikzcd}$$

is commutative, where Ω_A^* is the dual of Ω_A, V is now the tangent space of $\mathrm{Hom}(A, \bullet)$, the top row is the linear transformation associated to η, the columns are the canonical isomorphisms and the bottom row is the composition of the dual of $\mathrm{d}\varphi$ with the canonical isomorphism between D and its bidual.

Now let us come back to our proof. There exists a unique isomorphism η' from $\mathrm{Hom}(\mathbb{Z}[X]/K, (\bullet \otimes \overline{\mathbb{Q}})^\times)$ to $\mathrm{Hom}(A, \bullet)$ such that

$$\begin{tikzcd} \mathrm{Hom}(\mathbb{Z}[X]/K, (\bullet \otimes \overline{\mathbb{Q}})^\times) \arrow[r, "\eta'"] \arrow[dr, "\eta"'] & \mathrm{Hom}(A, \bullet) \arrow[d, "\zeta"] \\ & \mathbf{G} \end{tikzcd}$$

is commutative, and a unique morphism μ from $\mathrm{Hom}(A, \bullet)$ to $(\bullet \otimes D)^\times$ such that

$$\begin{tikzcd} \mathrm{Hom}(A, \bullet) \arrow[r, "\mu"] \arrow[d, "\zeta"'] & (\bullet \otimes D)^\times \\ \mathbf{G} \arrow[ur] & \end{tikzcd}$$

is commutative, where the diagonal arrow is the inclusion. Similarly, there exists a unique isomorphism $\hat{\eta}'$ of algebraic groups over $\overline{\mathbb{Q}}$ from $\mathrm{Hom}(\mathbb{Z}[X]/K, \bullet^\times)$ to $\mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet)$ such that

$$\begin{tikzcd} \mathrm{Hom}(\mathbb{Z}[X]/K, (\bullet \otimes \overline{\mathbb{Q}})^\times)_{\overline{\mathbb{Q}}} \arrow[r] \arrow[d] & \mathrm{Hom}(A, \bullet)_{\overline{\mathbb{Q}}} \arrow[d] \\ \mathrm{Hom}(\mathbb{Z}[X]/K, \bullet^\times) \arrow[r, "\hat{\eta}'"] & \mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet) \end{tikzcd}$$

is commutative, where the columns are the canonical isomorphisms and the top row is the map obtained from η' extending scalars to $\overline{\mathbb{Q}}$, and a unique morphism $\hat{\mu}$ from $\mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet)$ to $(\bullet \otimes \overline{\mathbb{Q}} \otimes D)^\times$ such that

$$\begin{tikzcd} \mathrm{Hom}(A, \bullet)_{\overline{\mathbb{Q}}} \arrow[r] \arrow[d] & (\bullet \otimes D)^\times_{\overline{\mathbb{Q}}} \arrow[d] \\ \mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet) \arrow[r, "\hat{\mu}"] & (\bullet \otimes \overline{\mathbb{Q}} \otimes D)^\times \end{tikzcd}$$

is commutative, where the columns are the canonical isomorphisms and the top row is the map obtained from μ extending scalars to $\overline{\mathbb{Q}}$. It is easy to check that

$$\begin{tikzcd} \mathrm{Hom}(\mathbb{Z}[X]/K, \bullet^\times) \arrow[r, "\sharp \circ \pi"] \arrow[d, "\hat{\eta}'"'] & \mathrm{Hom}(\mathbb{Z}[X], \bullet^\times) \arrow[d] \\ \mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet) \arrow[r, "\hat{\mu}"] & (\bullet \otimes \overline{\mathbb{Q}} \otimes D)^\times \end{tikzcd}$$

where the right column is the canonical isomorphism, is commutative. Also, let us denote by $\hat{S}$ the symmetric algebra on the dual of $\overline{\mathbb{Q}} \otimes D$, and let $\hat{\varphi}$ be the map given composition of

$$\hat{S} \to \overline{\mathbb{Q}} \otimes S \to \overline{\mathbb{Q}} \otimes A,$$

where the map on the left is the canonical isomorphism, and the map on the right is obtained from φ extending scalars to $\overline{\mathbb{Q}}$. Then

$$\begin{tikzcd}
\mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet) \arrow[r, "\sharp\circ\hat{\varphi}"] \arrow[d, "\hat{\mu}"] & \mathrm{Hom}(\hat{S}, \bullet) \arrow[d] \\
(\bullet \otimes \overline{\mathbb{Q}} \otimes D)^{\times} \arrow[r] & \bullet \otimes \overline{\mathbb{Q}} \otimes D
\end{tikzcd}$$

is commutative, too, where the right column is the canonical isomorphism and the bottom row is the inclusion. Also, there exists a unique structure of affine algebraic group over $\mathbb{Q}$ on $\mathrm{Hom}(A, \bullet)$ such that ζ is an isomorphism of algebraic groups. In turn, there exists a unique structure of affine algebraic group over $\overline{\mathbb{Q}}$ on $\mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet)$ such that the canonical natural isomorphism from $\mathrm{Hom}(A, \bullet)_{\overline{\mathbb{Q}}}$ to $\mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet)$ is an isomorphism of algebraic groups, and we have that the identity $\hat{\epsilon}$ of $\mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \overline{\mathbb{Q}})$ is the map obtained from the identity ϵ of $\mathrm{Hom}(A, \bullet)$ extending scalars to $\overline{\mathbb{Q}}$. Now let δ be a universal ϵ-differential of A with codomain Ω_A. Then the map $\hat{\delta}$ obtained from δ extending scalars to $\overline{\mathbb{Q}}$ is a universal $\hat{\epsilon}$-differential for $\overline{\mathbb{Q}} \otimes A$ with codomain $\overline{\mathbb{Q}} \otimes \Omega_A$. Also, let $\mathrm{d}\varphi$ denote the unique linear transformation from D^* to Ω_A such that

$$\begin{tikzcd}
S \arrow[r, "\varphi"] \arrow[d] & A \arrow[d, "\delta"] \\
D^* \arrow[r, "\mathrm{d}\varphi"] & \Omega_A
\end{tikzcd}$$

is commutative, where the left column is the canonical universal $\epsilon\circ\varphi$-differential of S with codomain D^*. Since $\mathbf{G}$ is connected, $\mathbb{Z}[X]/K$ is torsion free. Then exploiting results in the previous paragraph it is easy to see that

$$\begin{tikzcd}
\mathbb{Z}[X] \arrow[r, "\pi"] \arrow[d, "\psi"'] & \mathbb{Z}[X]/K \arrow[d] \\
\overline{\mathbb{Q}} \otimes D^* \arrow[r] & \overline{\mathbb{Q}} \otimes \Omega_A
\end{tikzcd}$$

is commutative, where the bottom row is the map obtained from $\mathrm{d}\varphi$ extending scalars to $\overline{\mathbb{Q}}$, the left column is given by composition of

$$\mathbb{Z}[X]/K \to W^* \to \overline{\mathbb{Q}} \otimes \Omega_A,$$

where in turn W^* is the dual of the tangent space of $\mathrm{Hom}(\overline{\mathbb{Q}} \otimes A, \bullet)$, the map on the left is the monomorphism associated to $\hat{\eta}'$ and the map on the right is the canonical isomorphism, and ψ is given by composition of

$$\mathbb{Z}[X] \to V^* \to (\overline{\mathbb{Q}} \otimes D)^* \to \overline{\mathbb{Q}} \otimes D^*,$$

where the map on the left is the monomorphism associated to the canonical isomorphism between $\mathrm{Hom}(\mathbb{Z}[X], \bullet^\times)$ and $(\bullet \otimes \overline{\mathbb{Q}} \otimes D)^\times$, and the other maps are the canonical isomorphisms. Also, it is easy to chech that ψ is the unique group morphism from $\mathbb{Z}[X]$ to $\overline{\mathbb{Q}} \otimes D^*$ sending any $x \in X$ to $\sum_{i=1}^n x(a_i) \otimes a_i^*$. Since the kernel of $\mathrm{d}\varphi$ is L, the thesis follows easily from these facts. $\square$

Now let $f_1, \ldots, f_l$ be a finite set of generators for the kernel of φ. It is easy to compute the images of $f_1, \ldots, f_m$ through δ, and of course they form a set of generators of L. Also, it is possible to compute F as well as the morphisms from D to it. For more information, see for example the online help of Magma. Once this has been done, it is easy to compute the kernel K of the previosly described morphism of abelian groups from $\mathbb{Z}[X]$ to $D^*/L \otimes F$. As $k_1, \ldots, k_m$, we can take any finite set of generators for K as an abelian group. Finally, there exist algorithms for computing the G_{k_i} and, in turn, the F_i. Again, more information can be found in the online help of Magma.

4.4 The big picture

Let $\mathbf{G}$ be a torus acting faithfully on a finite dimensional $\mathbb{Q}$-vector space V, and let L be a full-dimensional lattice of V. Also, let us denote by $\mathbf{G}_L$ the normalizer of L with respect to the action of the rational points of $\mathbf{G}$ on V. The action of $\mathbf{G}$ on V corresponds to a monomorphism of algebraic groups from $\mathbf{G}$ into GL_V. Composing it with the canonical isomorphism from GL_V to $(\bullet \otimes \mathrm{End}(V))^\times$, we obtain a monomorphism ι from $\mathbf{G}$ into $(\bullet \otimes \mathrm{End}(V))^\times$. Let us denote by $\widehat{\mathbf{G}}$ its image, and by χ the unique morphism of algebraic groups from $\mathbf{G}$ to $\widehat{\mathbf{G}}$ such that

$$\begin{tikzcd} \mathbf{G} \arrow[r, "\chi"] \arrow[dr, "\iota"'] & \widehat{\mathbf{G}} \arrow[d] \\ & (\bullet \otimes \mathrm{End}(V))^\times \end{tikzcd}$$

is commutative, where the vertical arrow is the inclusion. Of course it is even an isomorphism. Composing the inclusion of $\widehat{\mathbf{G}}$ into $(\bullet \otimes \mathrm{End}(V))^\times$ with the canonical isomorphism from $(\bullet \otimes \mathrm{End}(V))^\times$ to GL_V, we obtain a monomorphism which in turn corresponds to a faithful action of $\widehat{\mathbf{G}}$ on V. Let us denote by $\widehat{\mathbf{G}}_L$ the normalizer of L with respect to the action of $\widehat{\mathbf{G}}(\mathbb{Q})$ on V. In another direction, since $\widehat{\mathbf{G}}$ is in particular a subfunctor of $\bullet \otimes \mathrm{End}(V)$, by results of Section 4.1 we have that the subspace D of $\mathrm{End}(V)$ generated by $\widehat{\mathbf{G}}$ is a commutative and semisimple sub-$\mathbb{Q}$-algebra of $\mathrm{End}(V)$. The natural action of D on V gives by restriction an action of the group of units $D^\times$ of D on V. Let us denote by $D_L^\times$ the normalizer of L with respect to it. Then

Proposition 4.4.1. *We have that*

- *through the group isomorphism from $\mathbf{G}(\mathbb{Q})$ to $\widehat{\mathbf{G}}(\mathbb{Q})$ that χ associates to $\mathbb{Q}$, the image of $\mathbf{G}_L$ is $\widehat{\mathbf{G}}_L$, and that*
- *$\widehat{\mathbf{G}}_L$ is the intersection of $\widehat{\mathbf{G}}(\mathbb{Q})$ and of $D_L^\times$.*

Proof. It follows immediately from the definitions of $\widehat{\mathbf{G}}$, D, and their actions on V. $\square$

In particular,

Theorem 4.4.1. $\mathbf{G}_L$ *is finitely generated.*

Proof. By Proposition 4.2.1, we have that $D_L^\times$ is finitely generated. Therefore by the second part of Proposition 4.4.1 we have that $\widehat{\mathbf{G}}_L$ is finitely generated, too. Finally the thesis follows from the first part of Proposition 4.4.1. $\square$

Now let us denote by S the symmetric algebra on the dual of $\mathrm{End}(V)$, and let A be a finitely generated commutative $\mathbb{Q}$-algebra, η a natural isomorphism from $\mathrm{Hom}(A, \bullet)$ to $\mathbf{G}$ and φ a morphism from S to A such that A, η and φ are shadow data for $\mathbf{G}$ together with its action on V. Composing η and χ, we obtain an isomorphism η' from $\mathrm{Hom}(A, \bullet)$ to $\widehat{\mathbf{G}}$ such that A, η' and φ are shadow data for $\widehat{\mathbf{G}}$ and its action on V. Also, let us denote by S' the symmetric algebra on the dual of D, and by π the unique morphism from S to S' such that

$$\begin{tikzcd} \mathrm{End}(V)^* \arrow[r] \arrow[d] & D^* \arrow[d] \\ S \arrow[r, "\pi"] & S' \end{tikzcd}$$

is commutative, where the columns are the canonical inclusions and the bottom row is the dual of the inclusion of D into $\mathrm{End}(V)$. Then there exists a unique morphism φ' from S to A such that

$$\begin{tikzcd} S \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & S' \arrow[d, "\varphi'"] \\ & A \end{tikzcd}$$

is commutative, and it is such that

$$\begin{tikzcd} \mathrm{Hom}(A, \bullet) \arrow[r, "\sharp\circ\varphi'"] \arrow[d, "\eta'"] & \mathrm{Hom}(S', \bullet) \arrow[d] \\ \widehat{\mathbf{G}} \arrow[r] & \bullet \otimes D \end{tikzcd}$$

is commutative, too, where the bottom row is the inclusion and the right column is the canonical isomorphism.

In addition, let us suppose that A, η and φ are explicitely given. In particular, we have at hand a finite set of generators $f_1, \ldots, f_m$ for the kernel of φ. Therefore the discussion at the end of Section 4.1 shows how to compute D. In turn, according to the discussion concluding Section 4.2, we are able to compute a finite set of generators for $D_L^\times$. Also, the images of $f_1, \ldots, f_m$ through π form a finite set of generators for the kernel of φ', and of course computing them is just a matter of linear algebra. Therefore by results of Section 4.3 we are able to compute the splitting field F of D, the set X of morphisms from D to F, and, for every i between 1 and some integer m, subfields F_i of F, and integers $z_x^{(i)}$, where x ranges over the elements of X, such that there exist group morphisms ϕ_i from $D^\times$ to $F_i^\times$ sending $a \in D^\times$ to

$$\prod_{x \in X} x(a)^{z_x^{(i)}},$$

and with the property that $D_L^\times$ is the intersection of the $\ker\phi_i$. With an argument similar to the proof of Proposition 4.2.1, we have that elements in $D_L^\times$ are algebraic integers of D. Therefore it follows immediately that their images through ϕ_i are algebraic integers of F_i. Hence for every i between 1 and m we can apply Ge's algorithm to compute integral linear combinations of the previously computed finite set of generators of $D_L^\times$ for the elements of some finite set of generators of the kernel K_i of the composition of ϕ_i with the inclusion of $D_L^\times$ into $D^\times$. It follows from the second part of Proposition 4.4.1 that $\widehat{\mathbf{G}}_L$ is the intersection of the K_i. Therefore with the data we have at hand it is easy to compute a finite set of generators $g'_1, \dots, g'_n$ for it. Since the g'_i are elements of $\mathrm{End}(V)$ contained in the image of $\mathbf{G}(\mathbb{Q})$ through ι, in our hypothesis we are even able to compute elements g_i of $\mathbf{G}(\mathbb{Q})$ sent in g'_i by ι. By the first part of Proposition 4.4.1, $g_1, \dots, g_m$ generate $\mathbf{G}_L$. Therefore this discussion gives an algorithm for computing a finite set of generators for $\mathbf{G}_L$.

4.5 Numerical experiences

Let u_1, u_2, u_3, u_4 be the canonical basis of $\mathbb{Q}^4$, and let $\mathfrak{g}$ be the subspace of $\mathrm{End}(\mathbb{Q}^4)$ generated by the endomorphism x whose matrix with respect to u_1, u_2, u_3, u_4 is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -16 & 0 & 10 & 0 \end{pmatrix}.$$

Of course it is a sub-Lie-algebra of $\mathfrak{gl}(\mathbb{Q}^4)$. Therefore there exists a unique connected algebraic subgroup $\mathbf{G}$ of GL_4 such that $\mathfrak{g}$ is the Lie algebra of $\mathbf{G}$ and that the inclusion of $\mathfrak{g}$ into $\mathfrak{gl}(\mathbb{Q}^4)$ is the differential of the monomorphism from $\mathbf{G}$ into $\mathrm{GL}_{\mathbb{Q}^4}$ corresponding to the natural action of $\mathbf{G}$ on $\mathbb{Q}^4$. Exploiting the fact that x is semisimple, it can be shown that $\mathbf{G}$ is a torus. Also, we can use the methods described in [deG] to compute explicitely given defining polynomials for the unique algebraic matrix subgroup of $\mathrm{GL}_4(\mathbb{C})$ such that $\mathbf{G}(\mathbb{C}) = G$. With these data at hand, we can procede as explained in Section 2.4 to compute explicitely given shadow data for $\mathbf{G}$ together with its natural action on $\mathbb{Q}^4$. Therefore we can apply the algorithm described in Section 4.4 to compute a finite set of generators for $\mathbf{G}_{\mathbb{Z}^4}$. As a first thing, it turns out that the subalgebra D of $\mathrm{End}(\mathbb{Q}^4)$ generated by the image of $\mathbf{G}$ into $\bullet \otimes \mathrm{End}(\mathbb{Q}^4)$ has dimension 4, and it is the direct sum of two simple ideals E_1 and E_2, whose identities are the endomorphisms e_1 and e_2 of $\mathbb{Q}^4$ whose matrices with respect to u_1, u_2, u_3, u_4 are

$$\begin{pmatrix} -\frac{1}{3} & 0 & \frac{1}{6} & 0 \\ 0 & -\frac{1}{3} & 0 & \frac{1}{6} \\ -\frac{8}{3} & 0 & \frac{4}{3} & 0 \\ 0 & -\frac{8}{3} & 0 & \frac{4}{3} \end{pmatrix} \text{ and } \begin{pmatrix} \frac{4}{3} & 0 & -\frac{1}{6} & 0 \\ 0 & \frac{4}{3} & 0 & -\frac{1}{6} \\ \frac{8}{3} & 0 & -\frac{1}{3} & 0 \\ 0 & \frac{8}{3} & 0 & -\frac{1}{3} \end{pmatrix}.$$

In the notations of Section 4.2, we have that

$$x_1 = \frac{1}{6}u_1 + \frac{4}{3}u_3 \text{ and } x_2 = \frac{1}{6}u_2 + \frac{4}{3}u_4,$$

form a basis for L_1, and hence for V_1, and that

$$y_1 = \frac{1}{6}u_1 + \frac{1}{3}u_3 \text{ and } y_2 = \frac{1}{6}u_2 + \frac{1}{3}u_4.$$

are a basis for both L_2 and V_2. Of course, the faithful action of E_1 on V_1 corresponds to an embedding of E_1 into $\mathrm{End}(V_1)$. The image of $\mathcal{O}_1$ through it has a basis consisting of the endomorphisms whose matrices with respect to x_1, x_2 are

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 8 & 0 \end{pmatrix}.$$

Applying the algorithm by Pohst and Zassenhaus, we also find out that the image of $\mathcal{O}_1^\times$ into $\mathrm{End}(V_1)$ is generated by the automorphisms of V_1 whose matrices with respect to x_1, x_2 are

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 3 & 1 \\ 8 & 3 \end{pmatrix}.$$

In a similar way,

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

are the matrices with respect to y_1, y_2 of automorphisms of V_2 forming a generating set for the image of $\mathcal{O}_2^\times$ into $\mathrm{End}(V_2)$. Now with an easy computation we have that

$$3e_1 + e_1 x + e_2\ ,\ -e_1 + e_2\ ,\ e_1 + e_2 + e_2 x \text{ and } e_1 - e_2$$

are a finite set of generators for $D^\times_{L_1+L_2}$ and, applying the finite orbit stabilizer algorithm, that the automorphisms g_1, g_2 and g_3 of $\mathbb{Q}^4$ whose matrices are

$$\hat{g}_1 = \begin{pmatrix} -7 & -2 & 3 & 1 \\ -16 & -7 & 8 & 3 \\ -48 & -16 & 23 & 8 \\ -128 & -48 & 64 & 23 \end{pmatrix},\ \hat{g}_2 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

and

$$\hat{g}_3 = \begin{pmatrix} -23 & -16 & 3 & 2 \\ -32 & -23 & 4 & 3 \\ -48 & -32 & 7 & 4 \\ -64 & -48 & 8 & 7 \end{pmatrix}$$

are a finite set of generators for $D_L^\times$. Now the algorithm has to search for some group morphisms from $D^\times_{\mathbb{Z}^4}$ to the group of units of a number field such that the intersection of their kernels is the image of $\mathbf{G}_{\mathbb{Z}^4}$. It turns out that it is enough to consider just one morphism, namely

$$\chi : D_L^\times \to \mathbb{Q}[\sqrt{2}]$$

such that

$$\chi(g_1) = 12\sqrt{2} + 17\ ,\ \chi(g_2) = -1 \text{ and } \chi(g_3) = -408\sqrt{2} + 577.$$

Finally applying Ge's algorithm we find that the image of $\mathbf{G}_{\mathbb{Z}^4}$ is generated by $g_1^2 g_3$ and g_2^2. Since g_2^2 is the identity, it finally follows that $\mathbf{G}_{\mathbb{Z}^4}$ is the cyclic group generated by

$$\hat{g}_1^2 \hat{g}_3 = \begin{pmatrix} -215 & -84 & 99 & 36 \\ -576 & -215 & 276 & 99 \\ -1584 & -576 & 775 & 276 \\ -4416 & -1584 & 2184 & 775 \end{pmatrix}.$$

Despite the apparent simplicity of the input, the computation of $\mathbf{G}_L$ was definitely not a trivial task.

The algorithm described in Section 4.4 has been implement in Magma, and it has been tested in some non trivial cases. As an example, it has been executed on the algebraic subgroup of GL_m built as in the previous paragraph from the companion matrix of $X^m - 1$, for some integers m bigger than 1. It turns out that from a computational point of view the hardest part are the execution of the algorithm by Pohst and Zassenhaus and of the finite orbit stabilizer algorithm. However, the running times of the algorithm for m equal to 10, 11, 12 and 13 on a 2GHz processor with 1GB of memory for Magma are of 1862, 17.2, 169 and 1581 seconds, respectively. Therefore the whole algorithm is efficient enough to tackle non-trivial examples.

Chapter 5

Final remarks

In Chapter 2 we stated a problem concerning the algorithmic theory of algebraic groups which turned out to be equivalent to another problem previously considered by Grunewald and Segal, and for which the same authors had already provided an algorithm solving it in principle. The main contribution on this work was to provide, in Chapters 3 and 4, two original and practical algorithms solving the same problem in the special cases in which the algebraic group given in input is a unipotent group and a torus, respectively. Although these special cases have some interest in their own, finding a practical algorithm for solving the problem in the general case seems to be a much harder task. The next case to deal with could be the case of a connected solvable algebraic groups. The class of these groups contains properly both the class of unipotent algebraic groups and the class of the tori. Also, Lie-Kolchin theorem assures that if $\mathbf{G}$ is a connected solvable algebraic group acting faithfully on a finite dimensional vector space V, then there exists a flag

$$0 = V_0 < V_1 < \cdots < V_{n-1} < V_m = V$$

of $\mathbf{G}$-stable subspaces of V with the additional property that the image of the action of $\mathbf{G}$ on the V_i/V_{i+1} is a torus for every i between 1 and $m-1$, and such a flag can be easily computed using the Lie algebra of $\mathbf{G}$. Therefore a sharp refinement of the techniques employed in Chapters 3 and 4 is likely to lead to a practical algorithm for solving the problem in this more general case.

Bibliography

[AMD] Michael F. Atiyah, Ian G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BW] Thomas Becker and Volker Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[Bo] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1991.

[BHC] Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math. (2)*, 75:485–535, 1962.

[deG] Willem A. de Graaf. Constructing algebraic groups from their Lie algebras. Journal of Symbolic Computation. to appear 2008.

[DKD] Y. A. Drozd, V. V. Kirichenko, V. Dlab. *Finite-Dimensional Algebras.* Springer-Verlag Berlin and Heidelberg GmbH, 1994.

[EG] W. Eberly and M. Giesbrecht. Efficient decomposition of associative algebras. In Y. N. Lakshman, editor, *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation: ISSAC'96*, pages 170-178, New York, 1996. ACM

[Ei] Bettina Eick. Algorithms for polycyclic groups. Habilitation Thesis, Technische Universität Braunschweig, 2001.

[G4] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.10*, 2007. (`http://www.gap-system.org`).

[Ge] Guoqiang Ge. *Algorithms Related to Multiplicative Representations of Algebraic Numbers.* Ph.D. thesis, University of California at Berkeley, 1993.

[GS] Fritz Grunewald and Daniel Segal. Some general algorithms. I. Arithmetic groups. *Ann. of Math. (2)*, 112(3):531–583, 1980.

[GS2] Fritz Grunewald and Daniel Segal. Some general algorithms. II. Nilpotent groups. *Ann. of Math. (2)*, 112(3):585–617, 1980.

[Ma] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Mi] J.S. Milne. Algebraic Geometry. available at `http://www.jmilne.org/math/`.

[Mi2] J.S. Milne. Algebraic Groups and Arithmetic Groups. available at `http://www.jmilne.org/math/`.

[PZ] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory,* volume 30 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, 1989.

[Ro] Derek J. S. Robinson. *A Course in the Theory of Groups.*, volume 80 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1995.

[Si] Charles C. Sims. *Computation with finitely presented groups*, volume 48 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, 1994.

[Wa] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1979.